

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-256345

(43)Date of publication of application : 17.10.1990

---

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

H04N 1/44

---

(21)Application number : 01-077774

(71)Applicant : AISIN SEIKI CO LTD

(22)Date of filing : 29.03.1989

(72)Inventor : KATO EIJI

NARUSE YOSHIHIRO

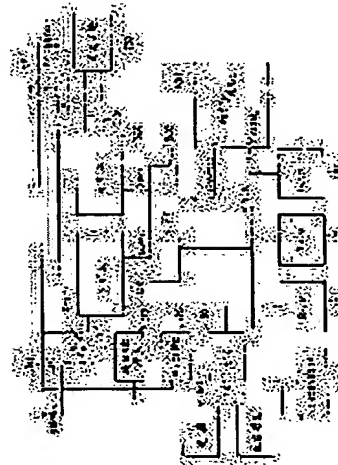
---

(54) PRIVACY COMMUNICATION CONTROLLER

(57)Abstract:

PURPOSE: To attain communication for plural number of times for transmission and reception of a key by disconnecting its own station side communication means from a communication line and transmitting and receiving the information relating to the key between privacy communication controllers connected to the communication line in that state.

CONSTITUTION: A memory card 130 is used as keys in a sense in privacy communication and freely attachable and detachable to/from a privacy equipment with a prescribed connector. The inside of the memory card 130 is provided with a battery for backing up the storage content and a read/write memory storing an ID code of the card. That is, only when the memory card having the same ID code is loaded to each privacy equipment arranged near a facsimile equipment at the sender side and the receiver side, normal privacy communication is attained.



---

## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

## ⑫ 公開特許公報(A) 平2-256345

⑮ Int.Cl.<sup>5</sup>

識別記号

庁内整理番号

⑯ 公開 平成2年(1990)10月17日

H 04 L 9/00

9/10

9/12

H 04 N 1/44

6940-5C

6945-5K

H 04 L 9/00

Z

審査請求 未請求 請求項の数 2 (全27頁)

⑰ 発明の名称 秘匿通信制御装置

⑱ 特 願 平1-7774

⑲ 出 願 平1(1989)3月29日

⑳ 発 明 者 加 藤 英 治 愛知県刈谷市朝日町2丁目1番地 アイシン精機株式会社  
内㉑ 発 明 者 成 瀬 好 廣 愛知県刈谷市朝日町2丁目1番地 アイシン精機株式会社  
内

㉒ 出 願 人 アイシン精機株式会社 愛知県刈谷市朝日町2丁目1番地

㉓ 代 理 人 弁理士 杉 信 興

## 明 細 書

## 1. 発明の名称

秘匿通信制御装置

## 2. 特許請求の範囲

(1) 相手側通信手段と接続される第1組の信号線；

前記第1組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第1の変復調手段；

自局側通信手段と接続された第2組の信号線；

第3組の信号線；

前記第3組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第2の変復調手段；

前記第1の変復調手段が復調した信号を暗号化して前記第2の変復調手段の変調入力端子に印加し、前記第2の変復調手段が復調した信号を

暗号化して前記第1の変復調手段の変調入力端子に印加する、秘匿情報処理手段；

前記第2組の信号線を、前記第1組の信号線と前記第3組の信号線との一方に選択的に接続する切換スイッチ手段；及び

自局側通信手段が発呼側か被呼側かを自動的に識別し、発呼側の時には、第1組の信号線上で被呼局識別の信号が検出された時に、被呼側の時には、自局側通信手段が被呼局識別の信号を送出する時に、前記切換スイッチ手段を制御して自局側通信手段を第1組の信号線から遮断し、暗号化通信の鍵を決定する暗号を含む情報の受渡しを、第1の変復調手段及び第1組の信号線を介して行ない、その後で、決定された鍵に基づいて、第1組の信号線に印加される暗号化された受信情報を前記秘匿情報処理手段に通し復号化して第2組の信号線に出力し、第2組の信号線からの送信情報を前記秘匿情報処理手段に通し暗号化して第1組の信号線に出力する、電子制御手段；  
を備える秘匿通信制御装置。

(2) 電子制御手段は、鍵を決定する暗号の受渡しにおいて：

自局側通信手段が発呼側の時には；乱数を生成し、生成した乱数をマスタ鍵で暗号化した情報を第1組の信号線に送出し、その後で第1組の信号線に現われる情報を受信して、受信した情報を前記乱数に基づいて解読し、解読した情報と前記乱数とが一致すると、前記乱数を以後の通信で暗号通信の鍵として利用し：

自局側通信手段が被呼側の時には；第1組の信号線に現われる情報を受信して、受信した情報をマスタ鍵で解読し、解読した情報をそれ自身に基づいて暗号化し、暗号化した情報を第1組の信号線に送出する、前記請求項1記載の秘密通信制御装置。

### 3. 発明の詳細な説明

#### 〔発明の目的〕

#### 〔産業上の利用分野〕

本発明は、例えば公衆通信回線を利用して画像情報を伝送するファクシミリ装置などの通信装置

その信号に関して同一の処理を行なうごく一部の装置、即ち自局と同一の機種しか相手側装置として利用できないという不都合がある。

また、秘密手段を、ファクシミリ装置自体に内蔵もしくは付加する構造であるため、秘密手段を備えるには、従来の装置をそのまま利用することはできず、ファクシミリ装置の改造や設計変更が必要不可欠である。

更に、非標準機能を示す信号(NSF)を利用する場合、この信号の通信装置間でのやりとりは、1往復のみしか許されていないという制約がある。秘密通信における暗号化/復号化に利用される鍵は、通信の度に変更するのが安全性の面で望ましく、その場合、送信側と受信側の鍵を一致させるために、鍵を設定する信号を、情報通信に先立って通信装置間で受渡しする必要がある。ところが、信号NSFを利用してその受渡しを行なう場合には、受渡しを一回しかできないので、実際に暗号化/復号化に使用する生の鍵コードを、NSF信号として直接、通信回線上に流さざるを得ない。

において、秘密通信を行なうために利用される秘密通信制御装置に関する。

#### 〔従来の技術〕

通信情報の暗号化/復号化の手段としては、従来より様々なものが提案されており、また、ファクシミリ装置においては、例えば秘密機能を備えるものとして、特開昭59-221167号の技術が知られている。

特開昭59-221167号の装置は、秘密機能をファクシミリ装置に内蔵するか、又は所定のインターフェースを介して、秘密装置をファクシミリ装置に外付けする構造になっている。また、秘密機能の有無を自動識別するために、CCITT勧告の通信制御手順に、オプション機能として規定される信号NSF(非標準機能を示す)を利用し、その信号に、秘密機能に関する情報を付加している。

#### 〔発明が解決しようとする課題〕

上述の装置においては、標準化されていない信号NSFによって秘密機能の識別を行なうので、

そのため、第三者が通信回線上を盗聴すれば、鍵コードを取出すことが可能であり、それに基づいて、後で送られる暗号化メッセージを解読することができるので、第三者に情報が漏れる恐れがある。

使用する鍵コード自体を暗号化して通信回線上に流せば、その漏洩の危険が小さくなる。しかし、通信回線上に生じたノイズなどの影響で、伝送中に情報に変形が生じる可能性もある。鍵コード自体を暗号化して受渡しする場合には、1往復の情報通信だけでは、確実に鍵コードの伝達が行なわれたか否かを確認することができず、正当な通信相手同志の間であっても受信側で正規の情報を解読できない場合が生じる。また、情報の変形によって鍵コードの受渡しに失敗した場合であっても、再送動作はできないので、一拒、回線を遮断して再び接続しない限り、正常な通信はできない。

本発明は、秘密通信における鍵コードを通信の度に更新する装置において、鍵の受渡しのための

複数回の通信を可能にすることを共通の課題とする。

〔発明の構成〕

〔課題を解決するための手段〕

上記課題を解決するため、本発明においては、相手側通信手段と接続される第1組の信号線；前記第1組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第1の変復調手段；自局側通信手段と接続された第2組の信号線；第3組の信号線；前記第3組の信号線と接続され、該信号線に現われる信号を復調し、変調入力端子に印加される信号を変調して前記信号線に出力する第2の変復調手段；前記第1の変復調手段が復調した信号を暗号化して前記第2の変復調手段の変調入力端子に印加し、前記第2の変復調手段が復調した信号を暗号化して前記第1の変復調手段の変調入力端子に印加する、秘匿情報処理手段；前記第2組の信号線を、前記第1組の信号線と前記第3組の信号線との一方に選択的に接続する切

ら自局側通信手段が切離され、その状態で通信回線に接続された秘匿通信制御装置同志の間で、鍵に関する情報のやりとりが行なわれる。従ってこの場合には、鍵に関する情報の受渡しを、実質上何回でも行なうことが可能である。このため、伝送路上における情報の変形などによって、鍵の情報の受渡しが失敗した場合、その受渡しのやり直しを、回線を切断することなく実行することができる。この情報の受渡しの際には、自局側及び相手側の通信手段（ファクシミリ）は、フェーズBに移行する前の待機状態であり、格別な不都合は生じない。

鍵の受渡しが完了した後は、その鍵に基づいて秘匿通信制御装置が、メッセージ情報の暗号化又は解読を行ないながらその中継を行なうことにより、秘匿通信を行なうことができる。

また、本発明の好ましい態様においては、使用される鍵コードが通信回線を盗聴する第三者に漏れるのを防止するために、鍵を決定する暗号の受渡しにおいて電子制御手段は、次のように処理す

換スイッチ手段；及び自局側通信手段が発呼側か被呼側かを自動的に識別し、発呼側の時には、第1組の信号線上で被呼局識別の信号が検出された時に、被呼側の時には、自局側通信手段が被呼局識別の信号を送出する時に、前記切換スイッチ手段を制御して自局側通信手段を第1組の信号線から遮断し、暗号化通信の鍵を決定する暗号を含む情報の受渡しを、第1の変復調手段及び第1組の信号線を介して行ない、その後で、決定された鍵に基づいて、第1組の信号線に印加される暗号化された受信情報を前記秘匿情報処理手段に通し復号化して第2組の信号線に出力し、第2組の信号線からの送信情報を前記秘匿情報処理手段に通し暗号化して第1組の信号線に出力する、電子制御手段；を設ける。

〔作用〕

本発明によれば、ファクシミリの通信プロトコルにおいて、CCITTによって規定されたフェーズAからフェーズBに移行する前に、切換スイッチ手段によって、通信回線（第1組の信号線）か

る。

自局側通信手段が発呼側の場合；

乱数を生成し、生成した乱数をマスタ鍵で暗号化した情報を第1組の信号線に送出し、その後で第1組の信号線に現われる情報を受信して、受信した情報を前記乱数に基づいて解読し、解読した情報と前記乱数とが一致すると、前記乱数を以後の通信で暗号通信の鍵として利用する。

自局側通信手段が被呼側の場合；

第1組の信号線に現われる情報を受信して、受信した情報をマスタ鍵で解読し、解読した情報をそれ自身に基づいて暗号化し、暗号化した情報を第1組の信号線に送出する。

この態様によれば、使用する鍵は暗号化された形で通信回線上に現われるので、それが第三者に盗聴されたとしても、鍵の漏洩によってメッセージが解読される恐れはない。

本発明の他の目的及び特徴は、以下の、図面を参照した実施例説明により明らかになる。

〔実施例〕

第1図に、実施例の秘匿装置を使用してファクシミリ通信を行なう場合の、通信系全体の構成を示す。

第1図を参照すると、互いに通信を行なうファクシミリ装置(FAX)は、交換機と接続される公衆電話回線に接続されており、該電話回線に接続された各々のファクシミリと交換機との間に、それぞれ、秘匿装置が介挿されている。ここに示した各々のファクシミリは、一般に市販されている、CCITTに規定されるG3のモードを備える装置であり、改造などは一切行なっていない。つまり、実施例の秘匿装置を電話回線上に介挿するだけで、既存のファクシミリ装置を用いて秘匿通信を行なうことができる。

第2図に、送信側と受信側にそれぞれ設けられる秘匿装置の構成の概要を示す。第2図を参照すると、送信側と受信側の秘匿装置は同一の構成になっている。即ち、各々の秘匿装置は、2つのモデム(変復調装置)、制御装置(CPU)、並びに信号のバイパス、暗号化及び復号化の機能を有

接続されている。また、リレーRY2の他方の接点には、秘匿装置内部の線路LiBが接続されている。この例では、リレーRY2がオフの時に回線LN1、LN2と回線LF1、LF2とが接続され、RY2がオンの時に回線LF1、LF2と線路LiBとが接続される。

更に、電話回線LN1、LN2はリレーRY1のノーマリオープン接点を介して、秘匿装置内部の線路LiAと接続されている。また、電話回線LN1、LN2には、極性反転検出回路210及び呼び出し検出回路220が接続されており、秘匿装置内部の線路LiBには電流供給回路230が接続されている。

秘匿装置のその他の構成要素としては、マイクロコンピュータ(CPU)100、ROM110、RAM120、メモ리카ード130、電源140、乱数発生回路150、入出力インターフェース(I/O)180、モデム300、400、バッファ回路500、暗号化/復号化処理回路600が備わっている。

するユニットを備えている。

秘匿通信を行なう場合、送信側においては、ファクシミリが回線上に送出した画像情報をモデムを介して入力し、それを暗号化した情報を別のモデムを介して回線上に送り出す。受信側においては、回線上に現われる暗号化情報をモデムを介して入力し、それを復号化して送信された画像情報を再生し、再生した情報を別のモデムを介してファクシミリに接続された側の回線上に送り出す。従って、各々のファクシミリは普通の動作を行なうだけであるが、2つの秘匿装置の間の回線上では、信号は暗号化されており、秘匿通信が行なわれることになる。

次に、第3図に示される秘匿装置の構成について説明する。交換機と接続される公衆電話回線LN1、LN2と、自局ファクシミリと接続される回線LF1、LF2との間には、リレーRY2が介挿されている。ファクシミリ側の回線LF1、LF2は、リレーRY2の共通接点に接続され、RY2の一方の接点に電話回線LN1、LN2が

2つのモデム300、400は、各々、CCITTのV27ter即ちG3規格に準拠した通信機能を備えている。

マイクロコンピュータ100のデータバスは、バッファ500を介してモデム300のデータバスDBM1とモデム400のデータバスDBM2に接続されている。従って、マイクロコンピュータ100は、モデム300を介して自局側のファクシミリと交信したり、モデム400を介して相手側のファクシミリと交信することができる。また、内部のデータバス(2)によって、バッファ500と暗号化/復号化処理回路600とが接続されている。バッファ回路500を制御することによって、データバス(2)は、モデム300のデータバスDBM1、又はモデム400のデータバスDBM2と接続できる。

従って、例えば自局側のファクシミリが送信を行なう場合、暗号化すべき画像情報は線路LiBからモデム300に入力されて復調され、データバスDBM1からバッファ500を通して、マイ

クロコンピュータ100のデータバスに現われ、暗号化／復号化処理回路600のXグループの端子に印加される。回路600は、Xグループの端子に印加されたデータを暗号化し、Yグループの端子を介してデータバス(2)に出力する。この暗号化されたデータは、バッファ500を通してデータバスDBM2に出力される。そして、モデム400によって変調され、線路LiAから電話回線LN1, LN2に送り出される。

逆に、自局側のファクシミリが受信を行なう場合、復号化すべき暗号化された画像情報は、線路LiAからモデム400に入力されて復調され、データバスDBM2からバッファ500を通して、データバス(2)に現われ、暗号化／復号化処理回路600のYグループの端子に印加される。回路600は、その情報を復号化、即ち解読し、解読した情報をXグループの端子に出力する。この情報は、マイクロコンピュータ100のデータバスを通り、バッファ500を通して、データバスDBM1を通りモデム300に印加される。モデム

ロコンピュータ100は、HD63B03Rである。ラッチLT1は、マイクロコンピュータ100のデータバスの信号として重畳された下位8ビットのアドレス情報(A7-A0)を抽出するアドレスラッチとして機能する。アドレスバスには、マイクロコンピュータ100が直接出力する上位の8ビット(AD15-AD8)アドレスラッチLT1の出力する下位8ビット(AD7-AD0)との16ビットの信号が現われる。

マイクロコンピュータ100に接続された各種周辺回路の各々の選択する各種チップセレクト信号は、デコーダDE2と各種論理ゲート(G5, G6, G7, G8, G9)で構成されるアドレスデコーダによって生成される。つまり、周辺回路の各々に予め割り当てられたアドレスがアドレスバスに現われると、それに対応するチップセレクト信号がデコードされ、その信号がアクティブになる。

第5b図には、ROM110, RAM120及びメモリカード130が示されている。これらの

300は、その情報を変調し、線路LiBを介して、自局側のファクシミリの回線LF1, LF2に送り出す。

メモリカード130は、秘匿通信におけるある種の鍵として利用されるものであり、所定のコネクタにより、秘匿装置に対して着脱自在になっている。このメモリカード130は、内部に記憶内容保持用のバッテリーと、そのカードのIDコードを記憶した読み書きメモリを備えている。つまり、送信側と受信側のファクシミリの近傍に配置される各々の秘匿装置に、同一のIDコードを有するメモリカードが装着されている場合にのみ、正常な秘匿通信が可能になる。

続いて、各回路の構成を更に詳細に説明する。第3図の各回路の詳細を、第5a図、第5b図、第5c図、第5d図、第6a図、第6b図、第7a図、第7b図、第8図及び第9図に示す。

まず、第5a図を参照して説明する。この回路には、マイクロコンピュータ100とその周辺回路要素が備わっている。ここで用いているマイク

回路は、アドレスバス、データバス及びコントロールバスを介して、マイクロコンピュータ100と接続されている。DE1はデコーダである。なお、メモリカード130は、図示しないコネクタにより、回路と着脱自在に接続されている。

第5c図には、入出力インターフェース180が示されている。この回路には、マイクロコンピュータ100のアドレスバス、データバス及びコントロールバスと接続された集積回路131と、そのポートに接続されたスイッチSW1-SW6, 発光ダイオードLED1-LED7, ブザーBZ, バッファ及びドライバが備わっている。

第5d図には、電源回路140と、乱数発生回路150が示されている。電源回路140は、商用交流電源(AC100V)の電力を直流の各種電圧に変換する機能を備えており、これ自体には格別新しい構成は備わっていない。

一方、乱数発生回路150は、アナログ電圧比較回路を構成している。2つの比較入力端子の一方の電圧は安定化されており、他方の入力端子に

は、電源回路140の出力する脈流電圧が印加される。この脈流電圧は、交流(50Hz)波形を全波整流したものを平滑化したものであり、その電圧は、常時微妙に変化しており、しかも電源ラインに混入した様々なノイズを含んでいる。アナログ電圧比較回路のしきい値レベルは、脈流信号のレベルが変化する範囲の中間的なレベルに設定してある。

このため、該比較回路の出力端子には、周期性の小さいパルス信号RMDが現われる。この信号RMDを順次サンプリングすることにより、サンプリングの周期にもよるが、ほぼランダムな乱数データが得られる。このようにして生成される乱数データは、この実施例では、秘匿通信を行なう際の鍵コードとして利用される。

次に、第6a図を参照する。この回路には、極性反転検出回路210、呼び出し検出回路220及びリレーRY1、RY2が示されている。リレーRY1及びRY2は、それぞれ、マイクロコンピュータ100の出力する信号NCU-RL1お

オン/オフする。電話回線LN1、LN2上の電圧の極性は、交換機によって反転されるので、その時の回線の極性を調べるために、この機能を設けてある。この機能は、回線LN1、LN2から自局側ファクシミリを切離し、秘匿装置に接続した時に、ファクシミリ側の回線LF1、LF2に供給する電圧の極性を、電話回線LN1、LN2と一致させるために利用される。

呼び出し検出回路220は、電話回線LN1、LN2上に現われる呼び出し信号を検出する機能を有する。呼び出し信号は交流信号なので、この回路においては、コンデンサによって直流成分を遮断した信号を全波整流回路に通して整流し、その整流出力に所定レベル以上の信号が現われる時に着呼信号がオンするように構成してある。

第6b図には、電流供給回路230が示されている。この回路は、自局側のファクシミリを電話回線LN1、LN2から切離して、秘匿装置側の線路L1Bに接続した時に、自局側のファクシミリ装置の回線LF1、LF2に電圧を供給する機

能を有する。電圧の極性をその時の電話回線LN1、LN2における極性と一致させるために、前述の極性反転検出回路210が出力する極性信号POL1及びPOL2を利用している。

極性反転検出回路210は、電話回線LN1、LN2を流れる電流の有無と電流の方向の識別を行なう。線路LN1の電流を検出するために、それぞれ、発光ダイオードとフォトトランジスタとで構成されるフォトカップラPC1及びPC2が備わっている。各フォトカップラの発光ダイオードは互いに逆極性で線路LN1上に介在されているので、一方の向きで電流が流れるとPC1がオンしてPC2がオフし、他方の向きで電流が流れるとPC1がオフしてPC2がオンする。電流が流れない時は2つのフォトカップラPC1、PC2は共にオフになる。

電話回線においては、受話機のフックがオンの時は回線に電流が流れず、フックがオフになると電流が流れる。従って、この実施例では、いずれかの方向に電流が流れていると、フックオフ信号がアクティブになるように構成してある。2つの信号POL1及POL2は、電流の向きに応じて

能を有する。電圧の極性をその時の電話回線LN1、LN2における極性と一致させるために、前述の極性反転検出回路210が出力する極性信号POL1及びPOL2を利用している。

従って、仮に既存のファクシミリ装置が、その接続された回線の電圧及び電流を監視して、その状態に応じた制御を行なっている場合でも、そのファクシミリの回線の接続を、電話回線からこの秘匿装置に切換えることによって何ら不具合が生じる恐れはない。なお、電話回線LN1、LN2においては、通常は48Vの電圧が現われるが、電流供給回路230は28Vの電圧を供給するようになっている。

第7a図には、モデム300が示されている。このモデムの回路の大部分は、シングルチップの集積回路(R48PCJ)310で構成されている。この集積回路310は、CCITTのV27terに準拠した機能を備えている。基本的には、集積回路310の機能として、そのデータ端子(D7-D0)に印加されるデジタル信号をシリ

アル信号に変換し変調を行なってシリアル送信出力端子TXOUTに出力する機能と、シリアル受信入力端子RXINに印加されるシリアル信号を復調しパラレルデータに変換してデータ端子(D7-D0)に出力する機能がある。

集積回路310のシリアル送信出力端子TXOUTから出力される信号は、信号処理回路320を通り、トランス330を通過して線路LiBに出力される。また、線路LiBから入力される信号は、トランス330を通り信号処理回路320を通過して、集積回路310のシリアル受信入力端子RXINに印加される。集積回路310のデータ端子(D7-D0)は、データバスDBM1に接続されている。

第7b図には、モデム400が示されている。このモデムの回路の大部分は、シングルチップの集積回路410で構成されている。この集積回路410は上記集積回路310と同一のものである。集積回路410のシリアル送信出力端子TXOUTから出力される信号は、信号処理回路420を

通り、トランス430を通過して線路LiAに出力される。また、線路LiAに入力される信号は、トランス430を通り、信号処理回路420を通過して、集積回路410のシリアル受信入力端子RXINに印加される。集積回路410のデータ端子(D7-D0)は、データバスDBM2に接続されている。

また、第7a図に示したモデム300が出力する割込要求信号IRQ1と、第7b図に示したモデム400が出力する割込要求信号IRQ2との論理和が、論理ゲートG15から出力され、それがマイクロコンピュータ100の割り込み要求入力端子INTに印加される。

第8図に、バッファ回路500を示す。第8図を参照すると、この回路は、各々双方向スリーステートバスバッファとして機能する、集積回路(74HC245)510、520及び530で構成されている。集積回路510のAグループの端子はモデム400のデータバスDBM2と接続され、集積回路520のAグループの端子はモデ

ム300のデータバスDBM1と接続され、集積回路530のAグループの端子はマイクロコンピュータ100のデータバスと接続されている。また、集積回路510、520、530の各Bグループの端子は、内部データバス(2)に共通に接続されている。

従って、集積回路510と530を制御することにより、マイクロコンピュータ100のデータバス、内部データバス(2)、及びモデム400のデータバスDBM2との3者の間で、いずれの方向にもデータを伝送することができ、また集積回路520と530を制御することにより、マイクロコンピュータ100のデータバス、内部データバス(2)、及びモデム300のデータバスDBM1との3者の間で、いずれの方向にもデータを伝送することができる。

第9図には、暗号化／復号化処理回路600の具体的な構成が示されている。第9図を参照すると、この回路は大きく分けて、鍵コード保持回路610、暗号化回路620及び復号化回路630

で構成されている。

まず、鍵コード保持回路610を説明する。この回路は、PROM(プログラマブルROM)611と2つのラッチ612、613で構成されている。PROM611のアドレス端子(A0~A7)に、マイクロコンピュータ100から、マスタ鍵の情報が印加される。PROM611には、各々のアドレスに互いに異なる鍵コードが予めストアしてあり、アドレス情報を与えることにより、そのアドレスに存在する8ビットの鍵コードを、データ端子(D0~D7)に出力する。

ラッチ制御信号KLT1及びKLT2を制御することにより、PROM611が出力する情報を、それぞれ、ラッチ612及び613に保持することができる。ラッチ制御信号KLT1を出力する時とKLT2を出力する時とで、PROM611に与えるマスタ鍵を変えることにより、ラッチ612に保持されるデータとラッチ613に保持されるデータとが異なる値になる。ラッチ612に保持された8ビットデータは、鍵コードKAとし



て、ラッチ613に保持された8ビットデータは鍵コードKBとして、それぞれ、暗号化回路620及び復号化回路630に印加される。

次に暗号化回路620を説明する。この回路は、4ビット全加算器621、622、排他的論理和(イクスクルーシブオア)回路623、624、及びスリーステート出力のバッファ625で構成されている。全加算器621のAグループの入力端子には、データバスを介して、暗号化すべき情報Xの下位4ビットの情報(X0-X3)が印加され、Bグループの入力端子には、鍵コードKAの下位4ビット(K0-K3)が印加される。また、全加算器622のAグループの入力端子には、データバスを介して、暗号化すべき情報Xの上位4ビット(X4-X7)が印加され、Bグループの入力端子には、鍵コードKAの上位4ビット(K4-K7)が印加される。全加算器621のキャリー出力は、全加算器622の入力端子に印加される。

全加算器621及び622の各Eグループの出

4ビット(K8-K11)が印加される。また、排他的論理和回路632のAグループの入力端子には、暗号化された情報Yの上位4ビット(Y4-Y7)が、内部データバス(2)から印加され、Bグループの入力端子には、鍵コードKBの上位4ビット(K12-K15)が印加される。

排他的論理和回路631及び632の各Eグループの出力端子から出力される信号は、それぞれ、全加算器633及び634のBグループの入力端子に印加される。全加算器633のAグループの入力端子には、鍵コードKAの下位4ビット(K0-K3)を各々反転した信号が印加され、全加算器634のAグループの入力端子には、鍵コードKAの上位4ビット(K4-K7)を各々反転した信号が印加される。

全加算器633が出力する4ビットの情報と全加算器634が出力する4ビットの情報は、バッファ635を介して、復号化された8ビットの情報Xとして、マイクロコンピュータ100のデータバスに出力される。

力端子は、それぞれ、排他的論理和回路623及び624のAグループの入力端子に印加される。また、排他的論理和回路623のBグループの入力端子には鍵コードKBの下位4ビット(K8-K11)が印加され、排他的論理和回路624のBグループの入力端子には鍵コードKBの上位4ビット(K12-K15)が印加される。

排他的論理和回路623の出力端子Yから出力される4ビットの信号及び624の出力端子Yから出力される4ビットの信号は、バッファ625を通過して、8ビットの暗号化情報Yとして、内部データバス(2)に出力される。

次に復号化回路630を説明する。この回路は、4ビット全加算器633、634、排他的論理和回路631、632、スリーステート出力のバッファ635及びインバータ群で構成されている。排他的論理和回路631のAグループの入力端子には、暗号化された情報Yの下位4ビット(Y0-Y3)が、内部データバス(2)から印加され、Bグループの入力端子には、鍵コードKBの下位

なお、上記暗号化回路620及び復号化回路630が行なう暗号処理の方法は、基本的には従来より知られているものである。それに関する説明は不要であろう。なお、第9図に示した暗号化/復号化処理回路600の処理の内容を簡略化したものを第4図に示すので参照されたい。

第10図に、この実施例で用いたメモ리카ード130の内部構造を示す。第10図を参照すると、このメモ리카ードには、読み書きメモリ(RAM)、バッテリー、制御回路及びコネクタ134が備わっており、コネクタ134によって、秘匿装置の本体に対し着脱自在になっている。コネクタ134の各端子には、電源ライン(Vcc)、カードセット信号端子(CST)、チップセレクト信号端子(CS)、書き込み制御出力(WPOUT)、書き込み制御入力(WE)、出力許可入力(OE)、アドレスバス(A0-A12)及びデータバス(D0-D7)が割当てられている。RAM131に、このメモ리카ード固有の(予め割当てられた)IDコードが格納されている。この実施例で

は、秘匿通信を行なうためには、同一のIDコードが書込まれたメモリカードが、送信側と受信側の双方の秘匿装置に必要である。

次に、実際の通信動作について説明する。通信を行なうファクシミリ装置の動作を、第11a図、第11b図、第11c図、第11d図、第11e図、第11f図及び第11g図に示し、秘匿装置の動作を第12a図、第12b図、第12c図、第12d図、第12e図、第12f図、第12g図、第12h図、第12i図、第12j図及び第12k図に示す。なお、ファクシミリ装置自体の処理の内容は、従来の装置と同一であるので、その部分については簡単に説明する。

以下、各図を参照して処理の内容を説明するが、その説明においては、第1図に示されるように、通信系が構成されているものとする。また、以下の説明においては、通信処理で伝送する信号の記号(括弧内に示す)には、CCITTの勧告によって定められた略号を用いてある。更に、ファクシミリは発呼側も被呼側も自動モードで動作するも

のとして説明する。

発呼側のファクシミリでは、フックをオフし(受話器を上げる動作に相当する)、交換機からのダイヤルトーンを検出すると、相手局の番号をダイヤルする(第11a図参照)。

被呼側では、交換機からの呼び出し音(リング音)を検出すると、フックをオフし、続いてそれがファクシミリであることを示す被呼局識別信号(CED)を回線に送出する。発呼側では、この信号(CED)を検出するまで、発呼側がファクシミリであることを示す発呼トーン(CNG)を回線に送出し続ける。

発呼側では、信号(CED)を検出後、ファクシミリの通信モードに入る。被呼側では、信号(CED)を送出後、被呼装置がCCITTの標準能力を有することを示す、デジタル識別信号(DIS)を送出する。つまり、信号(DIS)によって被呼側のファクシミリがどのモードの(G1, G2, G3等)通信能力があるかを発呼側に知らせる。

発呼側では、被呼側から送信されたデジタル識別信号(DIS)の内容から、自局ファクシミリの通信能力と合うかどうかをチェックし、双方の通信能力に合った通信モードを決定し、DIS信号に応答するデジタル命令信号(DCS)を被呼側に返送する。それに続いて、回線の状態をチェックする為にトレーニングチェック信号(TCF)を送信する。被呼側では、信号(DCS)を受けた後、指定されたモードで信号(TCF)を受信し、その受信結果を示す信号(CFR又はFTT)を返送する。

発呼側では、返送された受信結果により、通信状態が良好なら、次のメッセージ送信ステップに移り、状態が悪ければ通信モードを変更して(一般には通信速度を下げて)、再度信号(TCF)を送出する。

発呼側で信号(CFR)を受信すると、トレーニング信号を送出し、被呼側に同期をとらせ、続いてメッセージを送信する。被呼側では、トレーニング信号で同期をとった後、メッセージを受信

する。

被呼側では、発呼側が1頁の原稿を送信後、その終りを示すために送出する信号(RTC)を検出するまで、受信を続ける。

1頁の原稿を送信すると、発呼側では、最終原稿かどうかを検出し、最終原稿でなければ、マルチページ信号(MPS)を送った後、受信側から送出される受信確認信号(MCF)又は再トレーニング信号(RTP, RTN)を受信する。そして、受信した信号により、送信モードを変更するか、トレーニング送出か、又は回線切断かを選択する。

最終原稿である場合、割り込みによる手順の中断が入り、モード変更するか否かを識別し、モード変更しない場合には、手順終了信号(EOP)を送出後、回路切断動作に入る。モード変更する場合には、信号(MCF, RTP, RTNのいずれか)を受信すると、デジタル識別信号(DIS)を受信するまで待つ。

被呼側では、発呼側からの信号(MPS),

(EOP), (EOM:メッセージ終了)のいずれかを受信すると、信号(MCF), (RTP), (RTN)のいずれかで応答した後、命令受信状態に戻る。それ以外は回路切断動作に入る。

次に、秘匿装置の動作を説明する。

まず最初に、自局のファクシミリが発呼側と被呼側のいずれに属するかを識別する。つまり、第12a図において、ステップA52で、呼び出し検出回路220の出力する(着呼)信号をチェックし、ステップA55で、極性検出回路210の出力するフック信号をチェックし、着呼検出とフックオフ検出のいずれか先かを識別することによって、発呼側か被呼側かを検出する。被呼側であれば、まず最初に着呼信号が検出されるので、ステップA53でレジスタC<sub>1</sub>に1をストアする。発呼側であれば、着呼信号が検出されない時にステップA54でレジスタC<sub>1</sub>に0をストアし、フックオフが検出されるので、次の処理に進む。従って、以降の処理では、レジスタC<sub>1</sub>を参照することによって、自局のファクシミリが発呼側か被呼側か

を識別できる。

次に、秘匿装置にメモリカード130が装着されたか否かを識別する。これは、メモリカード130から出力されるカード装着信号CSTを参照することによって識別できる。発呼側と被呼側の少なくとも一方の秘匿装置にメモリカード130が装着されると、それによって秘匿通信の意志があるものとみなす。

メモリカード130が装着されると、ステップA59に進んでリレーRY1をオンし、ステップA60でレジスタC<sub>1</sub>の値をチェックし、発呼側又は被呼側の処理を行なう。

自局が被呼側の場合、ステップA69で、スイッチ(PAX-SW:SW1)をチェックし、自局のファクシミリのモードが手動か自動かを識別する。手動なら、ステップA70に進み、リレーRY2をオンにして、自局ファクシミリの回線LF1, LF2を秘匿装置内の線路LiBに接続し、ステップA71で、相手側、即ち発呼側の局に信号(CED)を送出する。

自局のファクシミリが自動モードなら、第12a図のステップG51に進む。そして、自局のファクシミリからの信号(CED)を検出すると、所定時間Tx<sub>2</sub>後に、リレーRY2をオンし、自局ファクシミリの回線LF1, LF2を秘匿装置内の線路LiBに接続する。

次に、秘匿スイッチ(SW2)の状態をチェックする。スイッチがオンなら、秘匿希望有とみなし、レジスタMrにACTCをストアし、そうでなければ、MrにNACTCをストアする。次に、ステップG61に進み、信号(DIS)が受信可能な状態に設定する。

次に、第12h図のステップH51に進み、レジスタMrの内容を、相手局に送出する。

ここで、自局が発呼側の場合を説明する。その場合、第12b図に示すステップB51に進み、まず信号(CED)を検出するまで待つ。この信号(CED)を検出すると、次にステップB56に進む。被呼側の局が通常のファクシミリであると、ここでDIS又はDTCが送られるが、被呼

側の局の秘匿装置が動作していると信号(CED)に続く、DIS又はDTCのかわりに、第12h図のステップH51で、Mrの内容が送られる。その場合、所定時間Tx<sub>2</sub>を経過すると、ステップB57からステップB58に進み、リレーRY2をオンして回線の接続を切換え、ステップB59で秘匿スイッチ(SW2)の状態を識別し、その結果に応じてレジスタMtの内容を設定する。そして、レジスタMrの内容が受信されるので、ステップB66から、第12c図のステップC51に進む。そして、レジスタMrとMtのいずれかがACTC、即ち秘匿希望であると、ステップC55に進む。

ステップC55では、乱数発生回路が出力する信号RDMのレベルを繰り返しサンプリングし、それによって乱数コードRを生成する。ステップC56では、生成された乱数コードRを、暗号化/復号化処理回路600の入力Xとして与えるとともに、メモリカード130から得たIDコードをマスタ鍵として暗号化/復号化処理回路600

に与え、該マスタ鍵に対応する鍵コードKA及びKBを生成し、乱数Rを暗号化した情報Ctを生成する。次のステップC57では、コードACTCに暗号Ctを付加した情報Xtを、被呼側の局に送出する。

被呼側の局では、第12b図のステップH52で、発呼局からの情報Xtを受信する。そして、XtがNACTCでなければ、ステップH56に進む。ステップH56では、被呼局のメモリカード130から得たIDコードをマスタ鍵として暗号化/復号化処理回路600に与え、該マスタ鍵に対応する鍵コードKA及びKBを生成する。そして、受信した暗号を暗号化/復号化処理回路600の暗号入力Yに与え、その暗号を解説する。解説した情報R'は、データベースに出力される。次のステップH57では、今度は解説した情報R'を、マスタ鍵として、暗号化/復号化処理回路600に与え、該マスタ鍵に対応する鍵コードKA、KBを生成する。そして、情報R'を暗号化/復号化処理回路600に入力情報Xとして入力し、

それを暗号化し、得られた暗号Xrを、発呼側の局に送出する。

発呼側の局では、ステップC58で暗号Xrを受信すると、ステップC59に進む。ステップC59では、暗号Xrを、暗号化/復号化処理回路600の暗号入力Yに入力するとともに、最初に送った乱数と同一の値をマスタ鍵として暗号化/復号化処理回路600に与え、暗号Xrを復号化する。このようにして復号化される情報R''は、
$$R'' = D_r(E_r'(R')) \quad \dots(1)$$

但し、R': 被呼側が解説したR

$E_r'$ : 被呼側の暗号化の関数

$D_r$ : 発呼側の復号の関数

であるから、発呼側と被呼側の暗号化及び復号化の条件が全て一致する場合には、R''は最初に送った乱数Rと等しくなる。もし、初呼側のメモリカードと被呼側のメモリカードに記憶されたIDコードが異なる場合には、RとR''とは一致しない。発呼局側はステップC60でRとR''とを比較し、それが一致すると、ステップC62に進み、レジ

スタRfに1をストアしてそれを被呼側に送出する。もし一致しない場合には、暗号の送出と返送される暗号との照合が3回繰り返される。3回の照合で一致しなければ、秘匿通信の動作は禁止される。

被呼側では、第12b図のステップH58で、Rfを受信すると、ステップH61以降の処理に進む。

上述のようにして秘匿通信が可能な状態になるまでの間は、被呼局側のファクシミリは、デジタル識別信号(DIS)を送出し続けており、発呼側のファクシミリはその信号を待ち続けている。そして、被呼局側の秘匿装置は、ステップH65に進むと、既に自局ファクシミリからのデジタル識別信号(DIS)を受信しているの、その信号を相手側(発呼側)の局に送信する。

このようにして秘匿通信が可能な状態になると、後は通常のファクシミリ通信と同様の手順で情報の伝送が行なわれるが、その場合、秘匿装置は自局側のファクシミリと相手局側(秘匿装置)との

データ伝送の仲介を行なうことになり、自局側のファクシミリが送信した情報は、秘匿装置を介して相手局に送られ、相手局から送られた情報は、秘匿装置を介して自局のファクシミリに送られる。画像情報に対しては、仲介する際に、暗号化又は復号化が行なわれる。その場合、暗号化すべき情報は、暗号化/復号化処理回路600の入力端子Xに印加され、復号化すべき情報は入力端子Yに印加される。また、暗号化/復号化処理回路600のマスタ鍵コードとしては、自局と相手局との間で既に転送され確認及び照合された、乱数がいずれの局においても使用される。つまり、秘匿通信で使用される鍵、即ち、セッション鍵には、通信の度に互いに異なる値が使用される。従って、極めて安全性が高い。

なお、上記実施例においては、算術加算と非他論理和の演算によって暗号化/復号化を行なっているが、暗号化の方式に関しては、従来より知られる他の様々な方法を用いても本発明は同様に実施しうる。例えば、ストリーム暗号のように、

鍵の値をカウントアップする方法により逐次更新する方法を用いてもよいし、暗号化した直前のデータを鍵として利用する方法を用いてもよい。

また、実施例では、ファクシミリ同志で通信を行なう場合の秘匿通信について説明したが、同様の通信手順で通信を行なう装置であれば、ファクシミリに限らず、本発明の装置を用いて、秘匿通信を行なうことが可能である。

#### 【効果】

以上のとおり、本発明によれば、ファクシミリの通信プロトコルにおいて、CCITTによって規定されたフェーズAからフェーズBに移行する前に、切換スイッチ手段によって、通信回線（第1組の信号線：LN1，LN2）から自局側通信手段が切離され、その状態で通信回線に接続された秘匿通信制御装置同志の間で、鍵に関する情報のやりとりが行なわれる。従ってこの場合には、鍵に関する情報の受渡しを、実質上何回でも行なうことが可能である。このため、伝送路上におけ

る情報の変形などによって、鍵の情報の受渡しが失敗した場合、その受渡しのやり直しを、回線を切斷することなく実行することができる。この情報の受渡しの際には、自局側及び相手側の通信手段（ファクシミリ）は、フェーズBに移行する前の待機状態であり、格別な不都合は生じない。

鍵の受渡しが完了した後は、その鍵に基づいて秘匿通信制御装置が、メッセージ情報の暗号化又は解読を行ないながらその中継を行なうことにより、秘匿通信を行なうことができる。

#### 4. 図面の簡単な説明

第1図は、実施例の秘匿装置を利用する通信系全体の構成を示すブロック図である。

第2図は、送信側と受信側に各々設けられた秘匿装置の構成の概要を示すブロック図である。

第3図は、実施例の1つの秘匿装置の構成を示すブロック図である。

第4図は、暗号化／復号化処理回路600の概略を示すブロック図である。

第5a図、第5b図、第5c図、第5d図、第

5e図、第5f図、第5g図、第5h図、第5i図、第5j図、第5k図、第5l図、第5m図、第5n図、第5o図、第5p図、第5q図、第5r図、第5s図、第5t図、第5u図、第5v図、第5w図、第5x図、第5y図、第5z図、第6a図、第6b図、第7a図、第7b図、第8図、第9図及び第10図は、第4図に示す各部の詳細構成を示すブロック図である。

第11a図、第11b図、第11c図、第11d図、第11e図、第11f図及び第11g図は、ファクシミリの通信処理の内容を示すフローチャートである。

第12a図、第12b図、第12c図、第12d図、第12e図、第12f図、第12g図、第12h図、第12i図、第12j図及び第12k図は、秘匿装置の動作を示すフローチャートである。

100：マイクロコンピュータ（電子制御手段）

110：ROM

120：RAM

130：メモリカード

134：コネクタ

140：電源

150：乱数発生回路

180：入出力インターフェース

210：極性反転検出回路

220：呼び出し検出回路

230：電流供給回路

300：モデム（第2の変復調手段）

310，410：集積回路

320，420：信号処理回路

330，430：トランス

400：モデム（第1の変復調手段）

500：バッファ回路

600：暗号化／復号化処理回路（秘匿情報処理手段）

610：鍵コード保持回路

611：PROM

612，613：ラッチ

620：暗号化回路

621，622：全加算器

623，624：排他的論理和回路

625：バッファ

630：復号化回路

631，632：排他的論理和回路

633，634：全加算器

635：バッファ

RY1：リレー

RY2：リレー（切換スイッチ手段）

LN1，LN2：公衆電話回線（第1組の信号線）

LF1，LF2：回線（第2組の信号線）

LiA：線路

LiB：線路（第3組の信号線）

LT1：ラッチ

DE1，DE2：デコーダ

SW1-SW6：スイッチ

LED1-LED7：発光ダイオード

BZ：ブザー

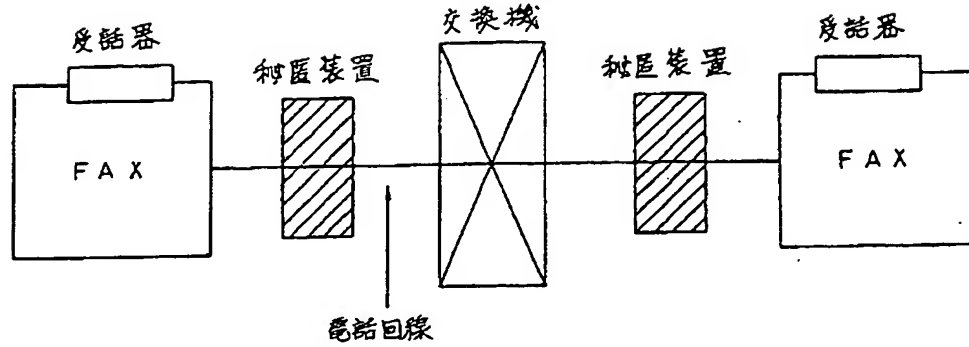
PC1，PC2：フォトカップラ

出願人 アイシン精機株式会社

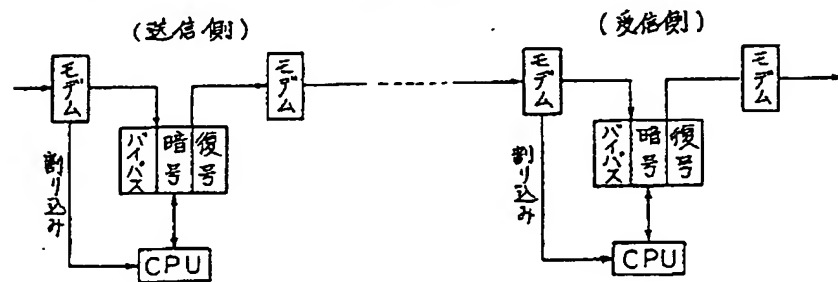
代理人 井理士 杉 信 興



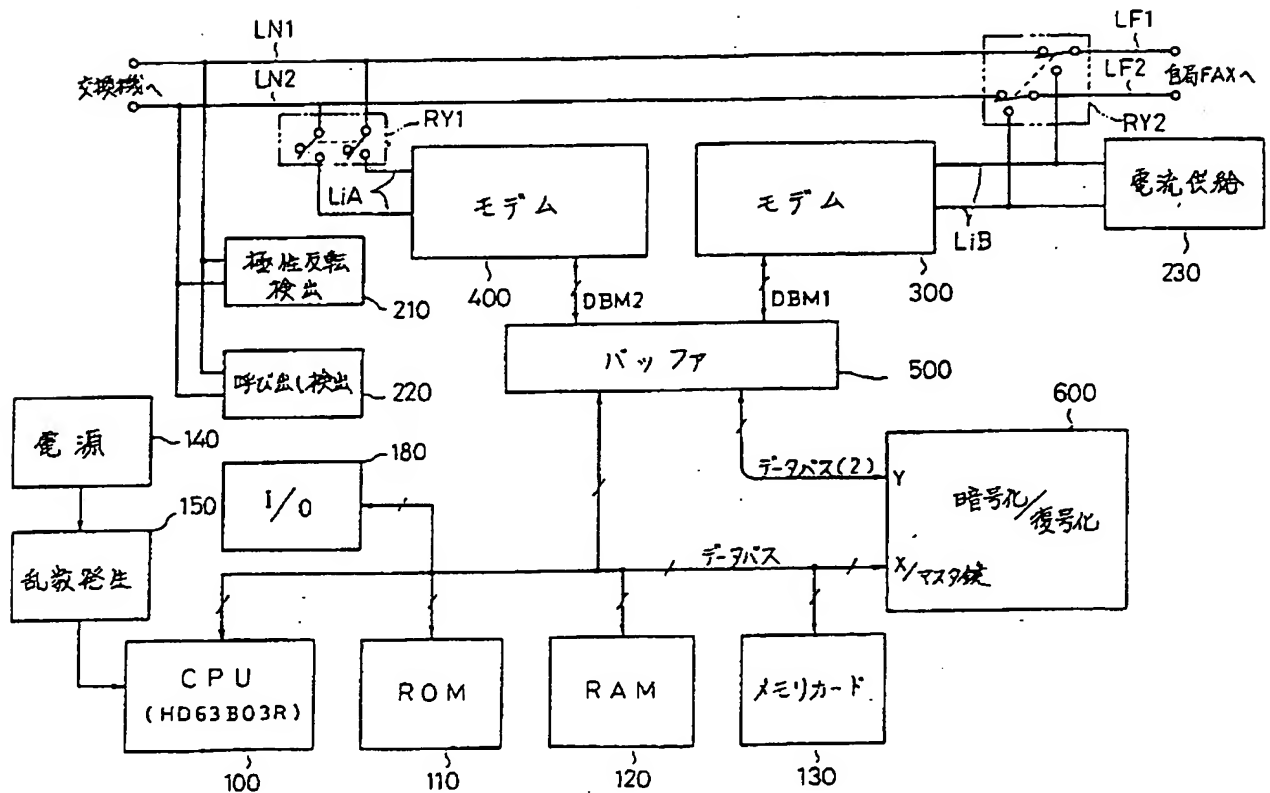
第 1 図



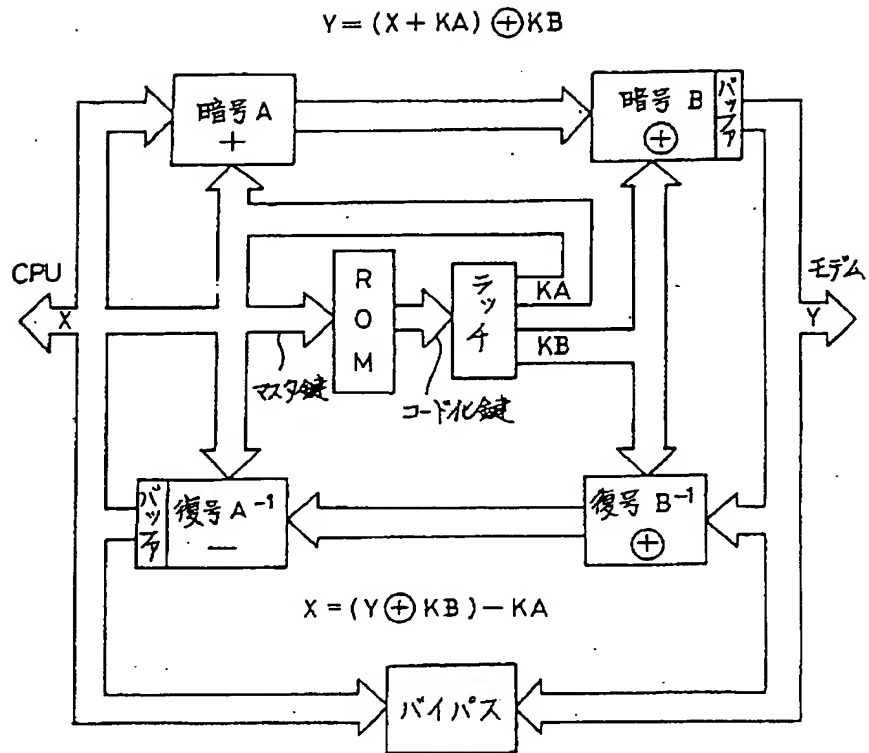
第 2 図



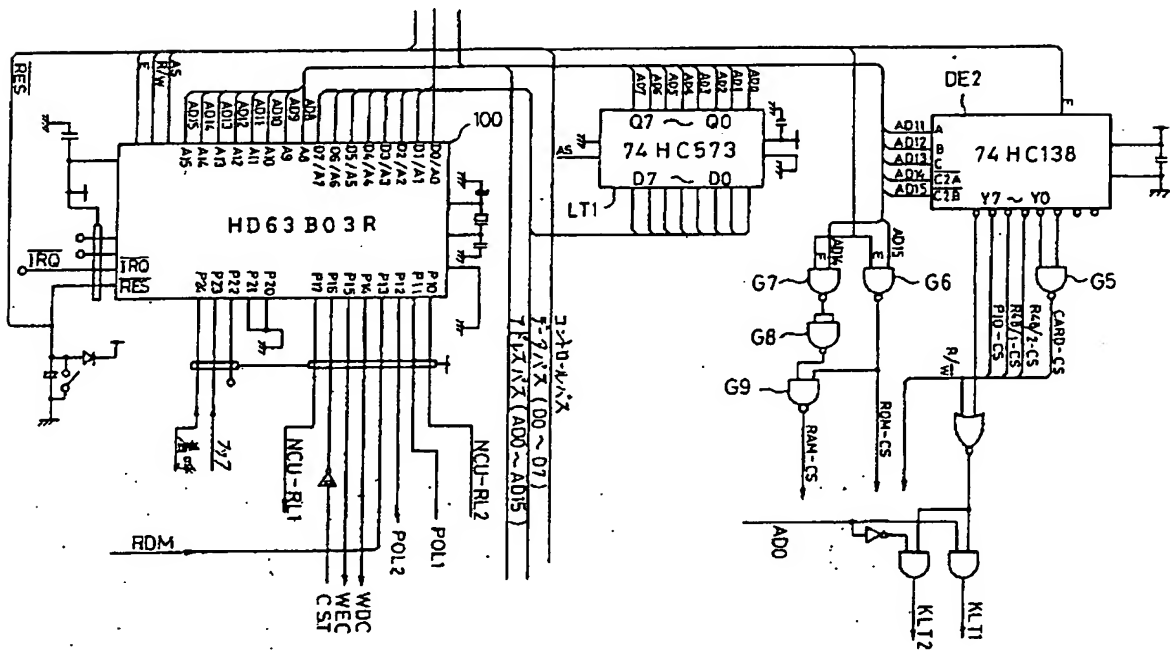
第 3 図



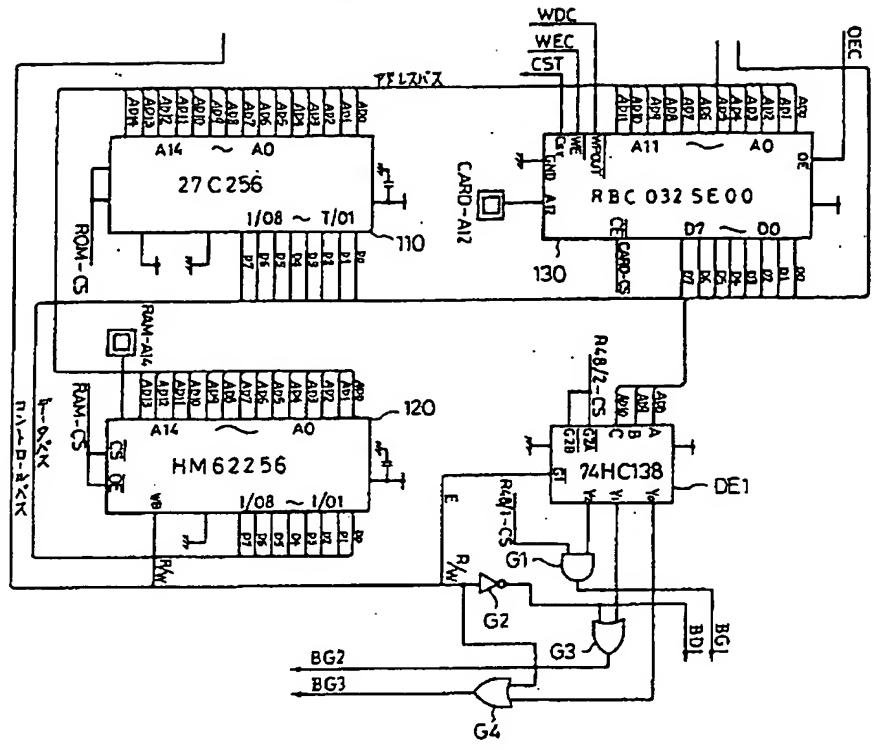
第 4 図



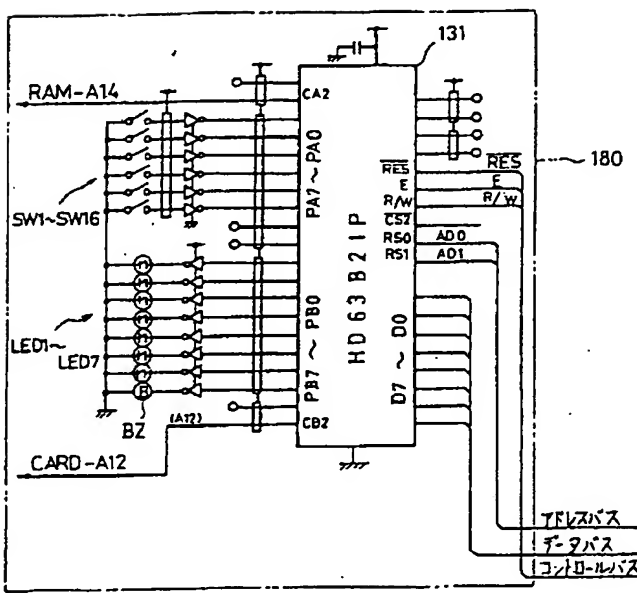
第 5a 図



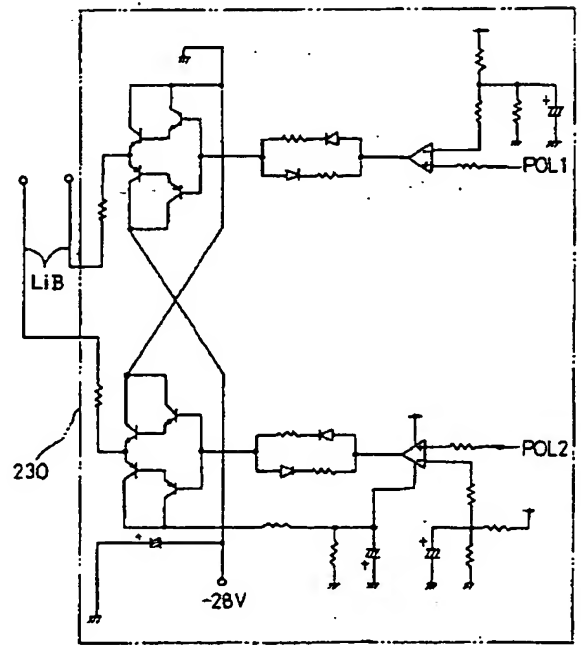
第 5b 図



第 5c 図

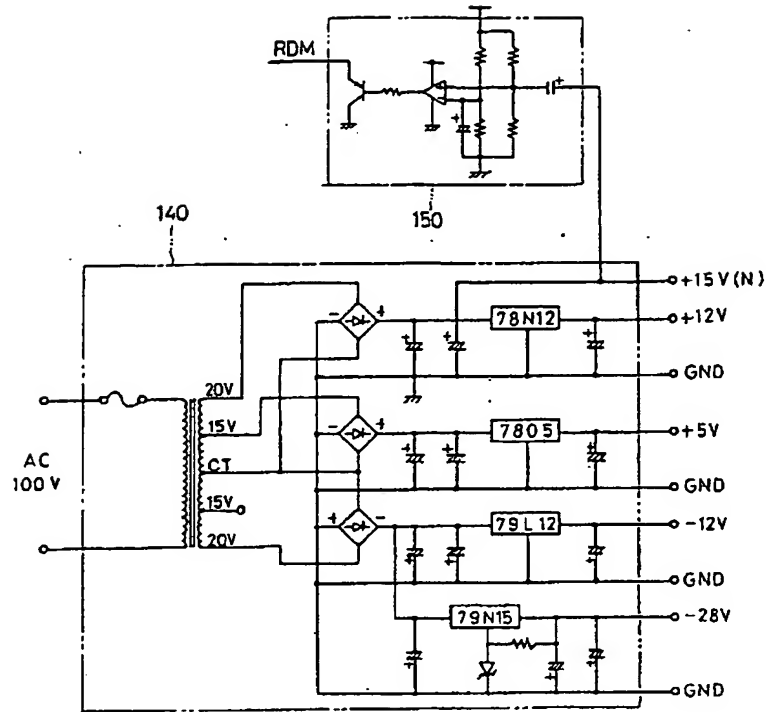


第 6b 図

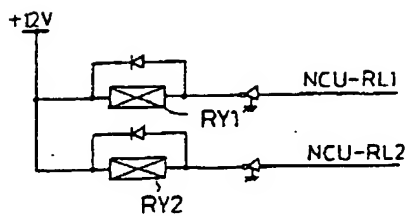
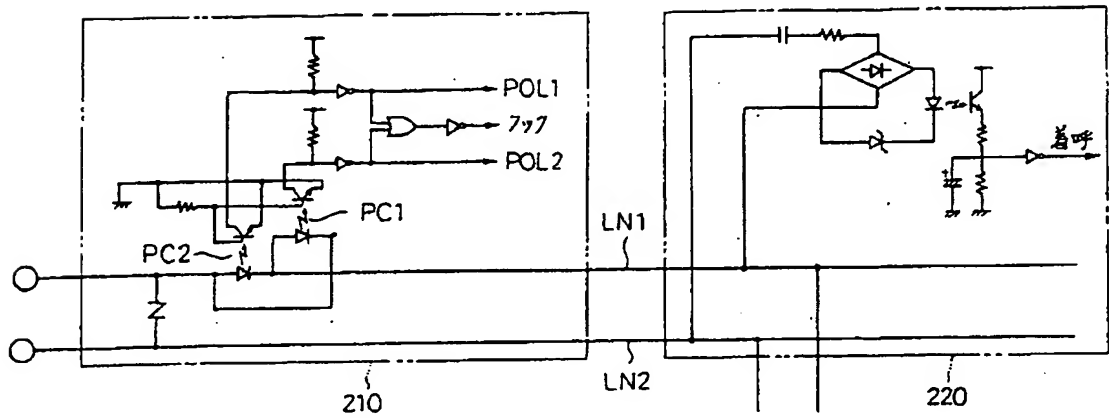




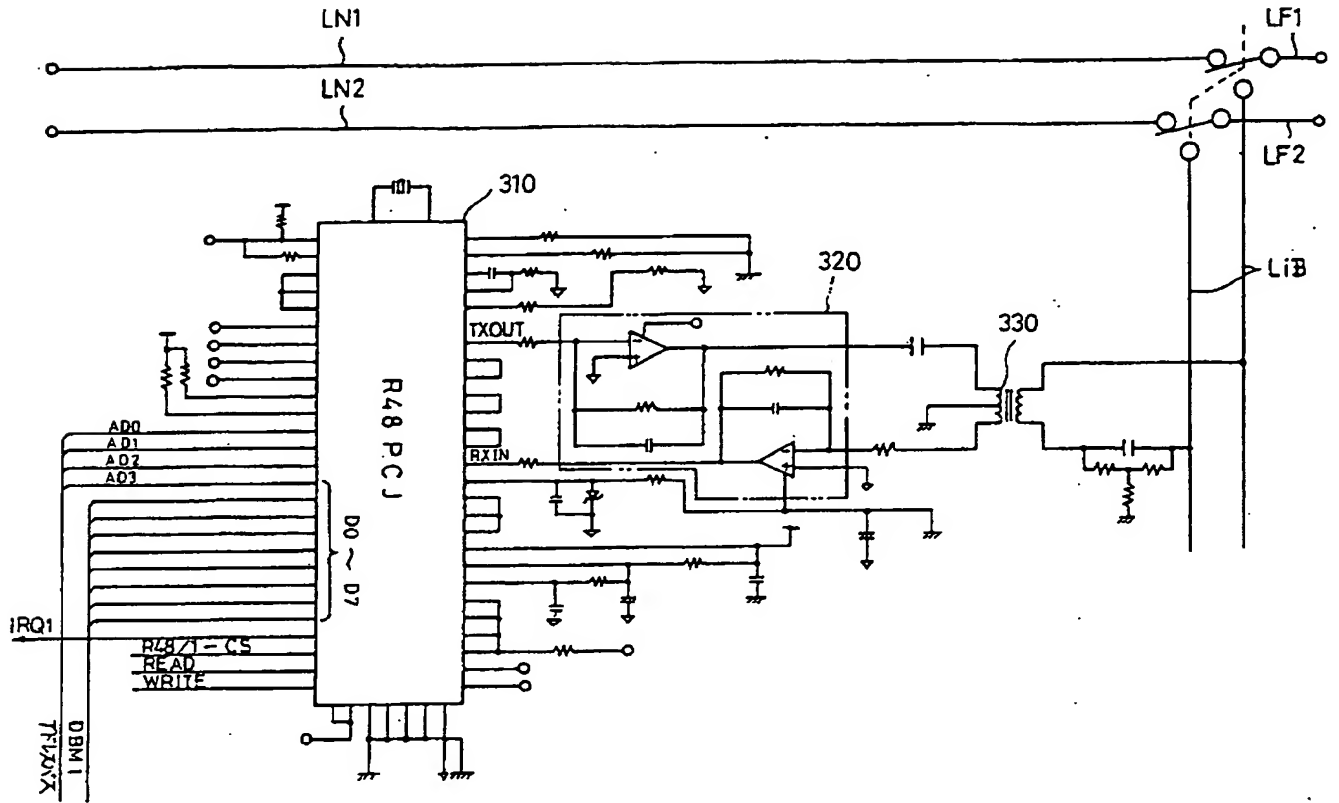
第5d図



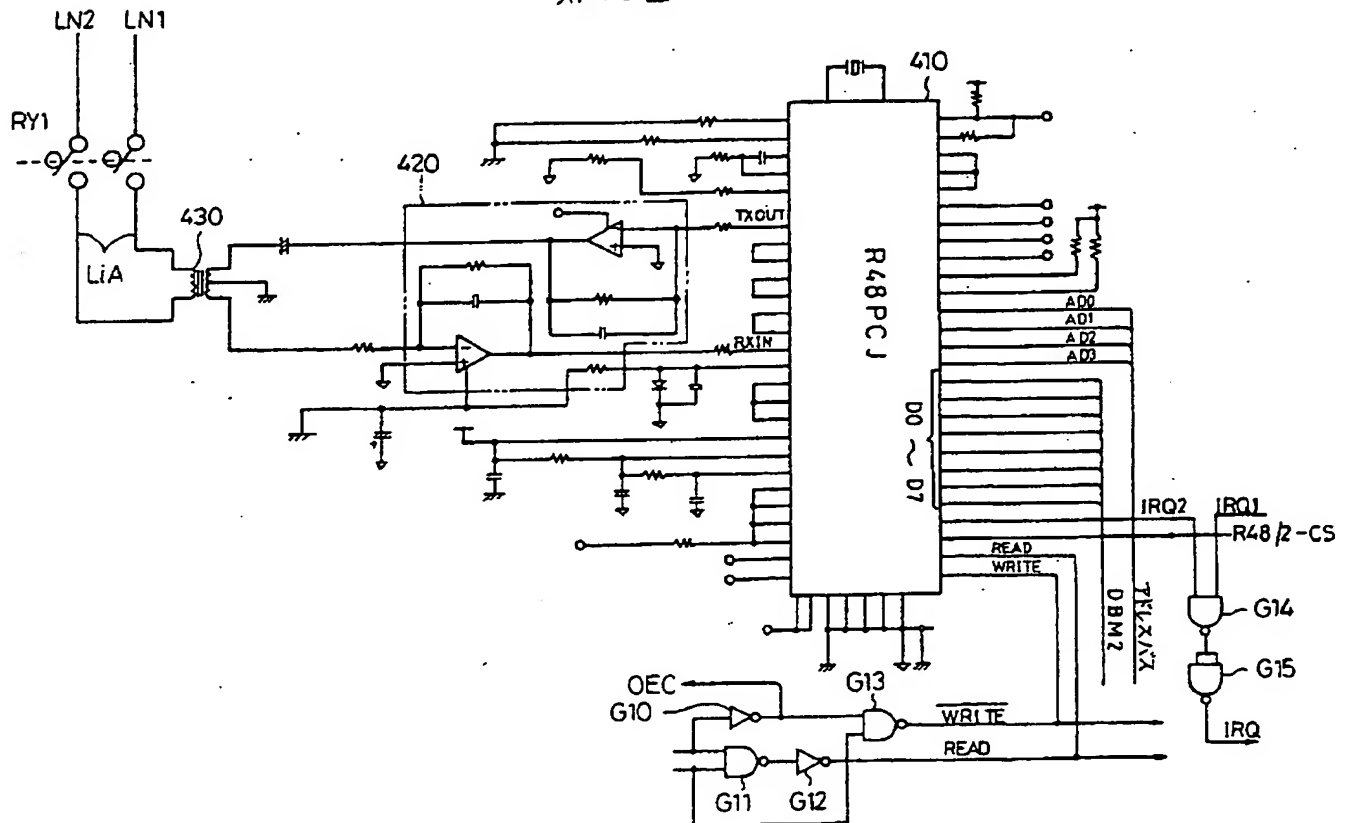
第6a図



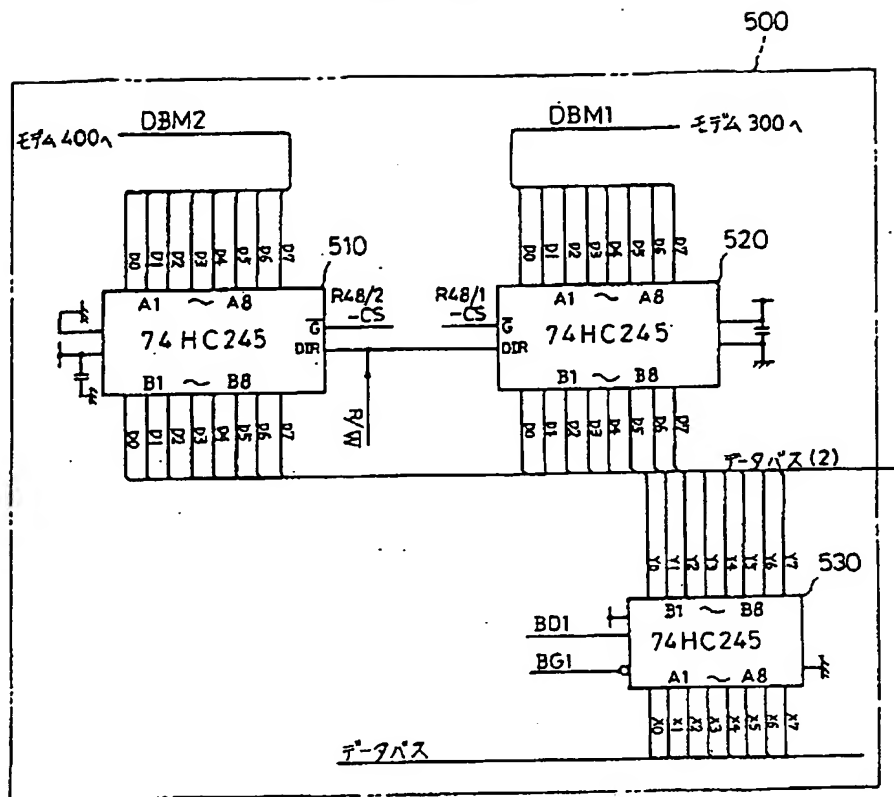
第 7a 図



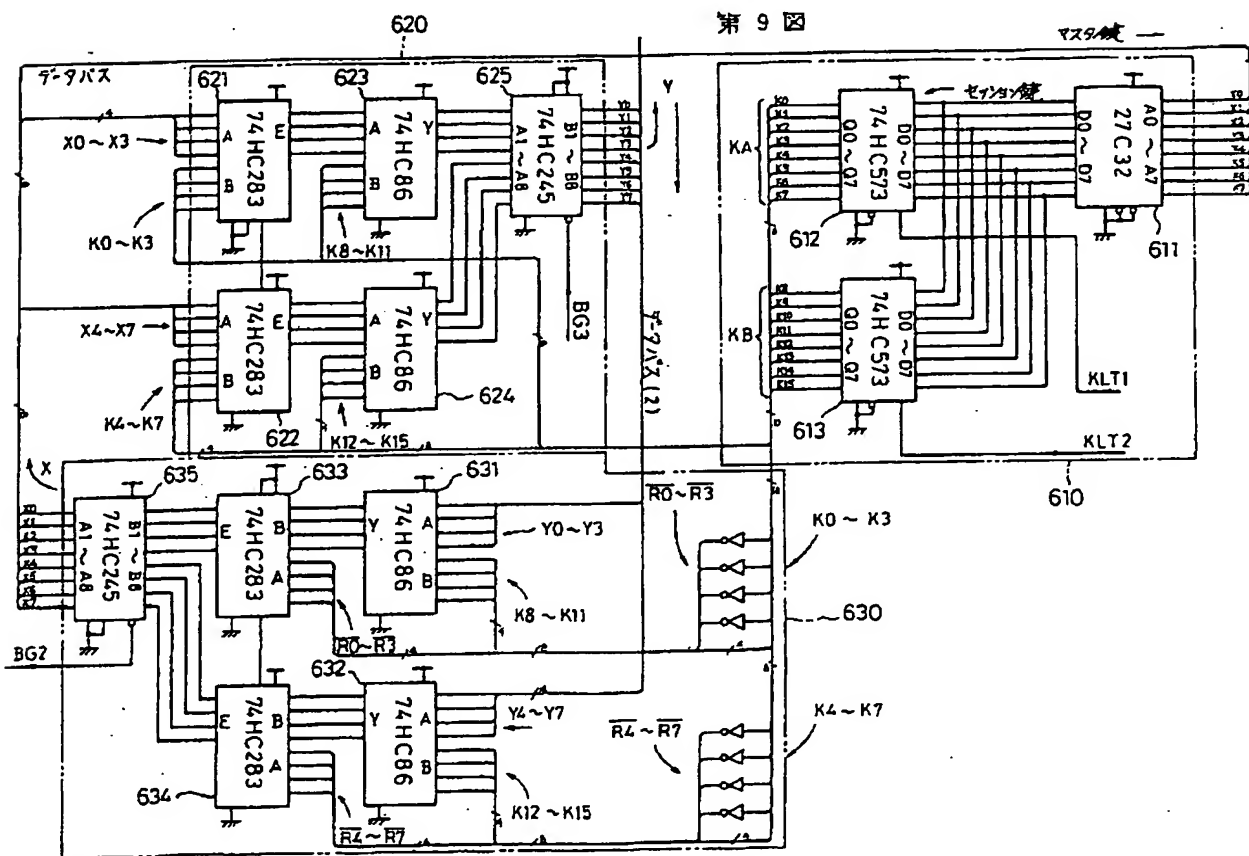
第 7b 図



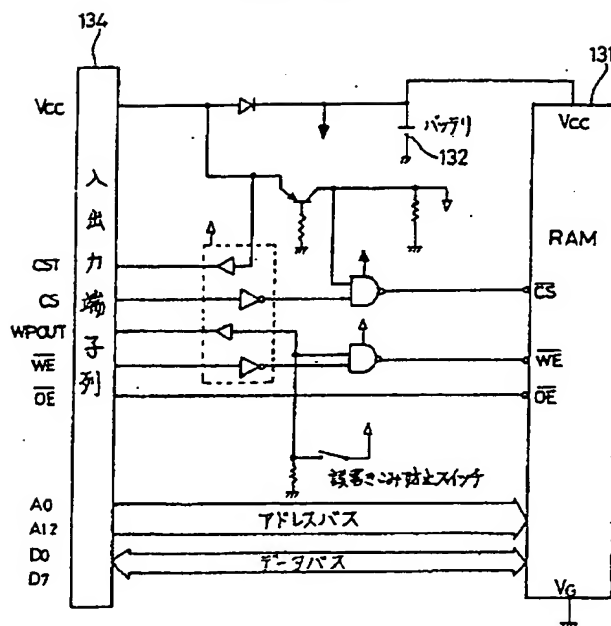
第 8 図



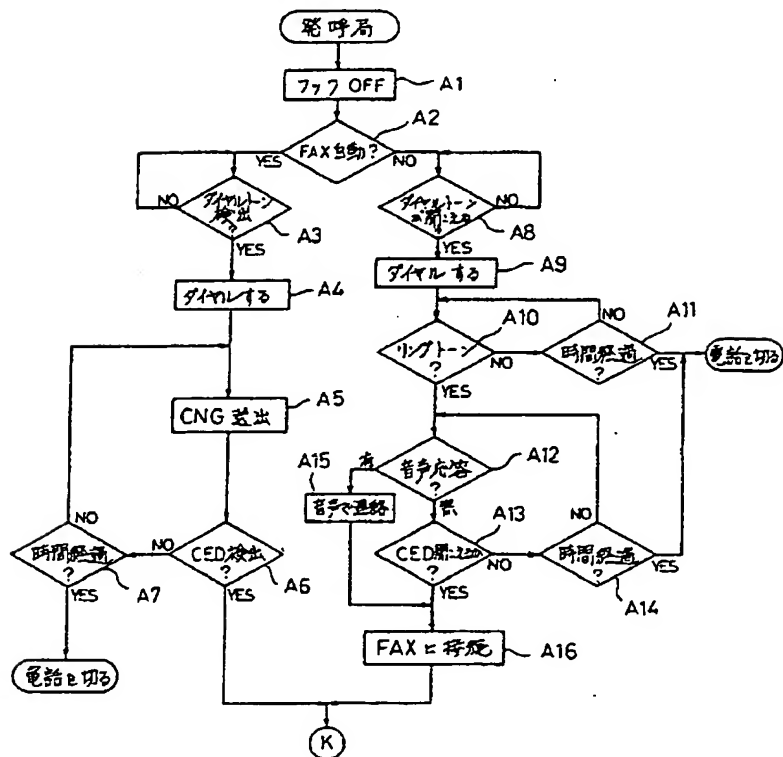
第 9 図



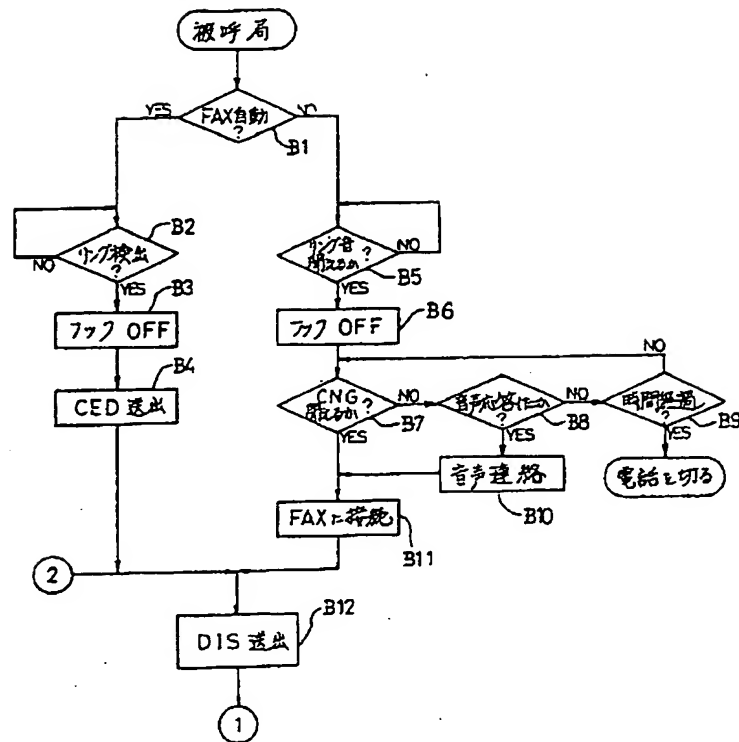
第 10 図



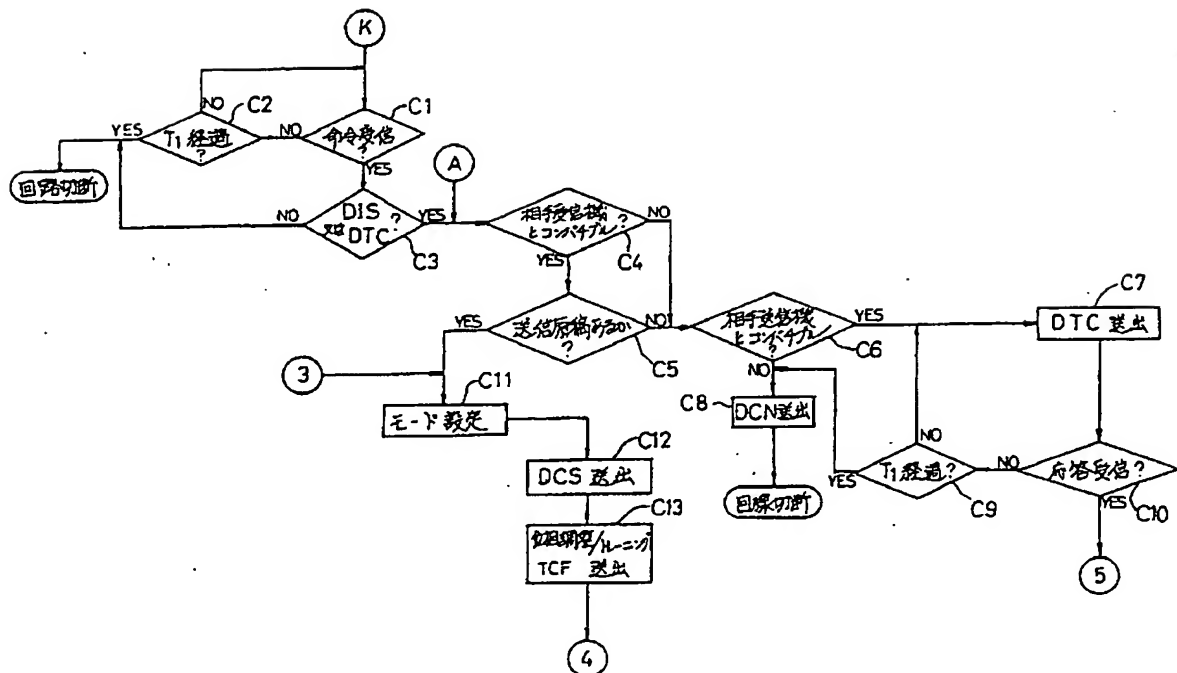
第 11a 図



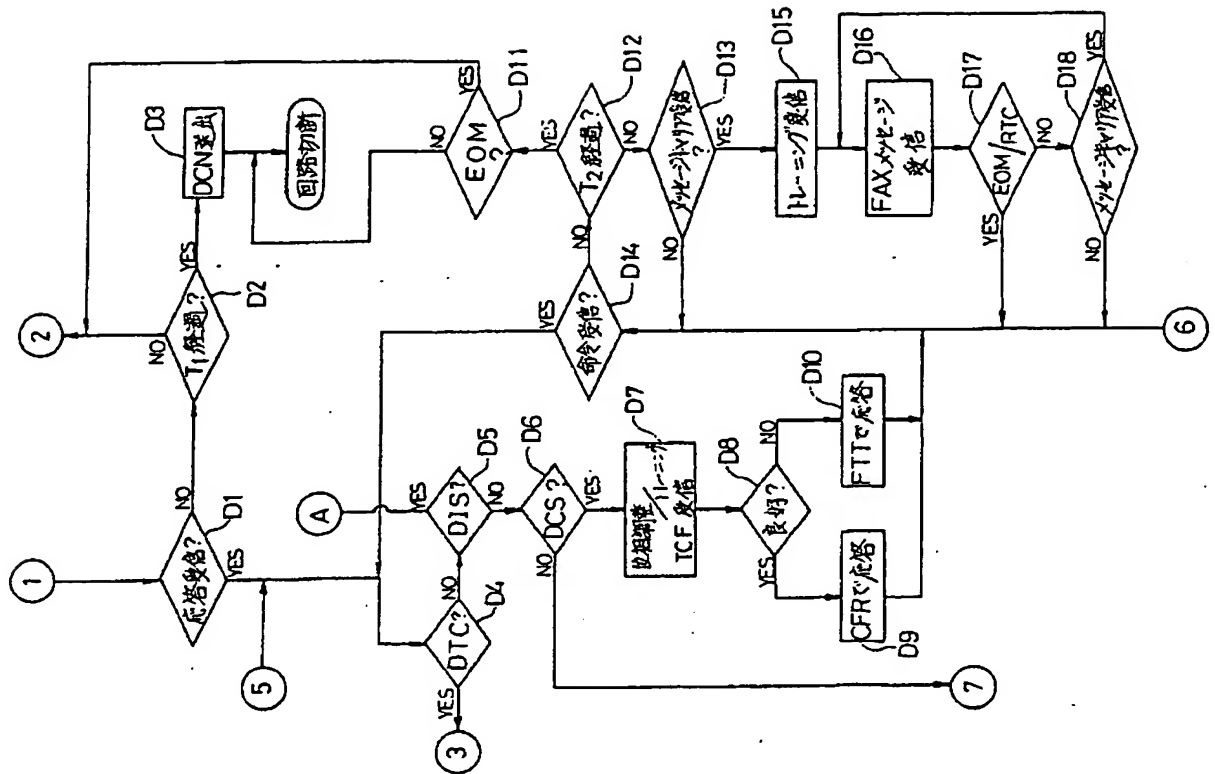
第 11b 図



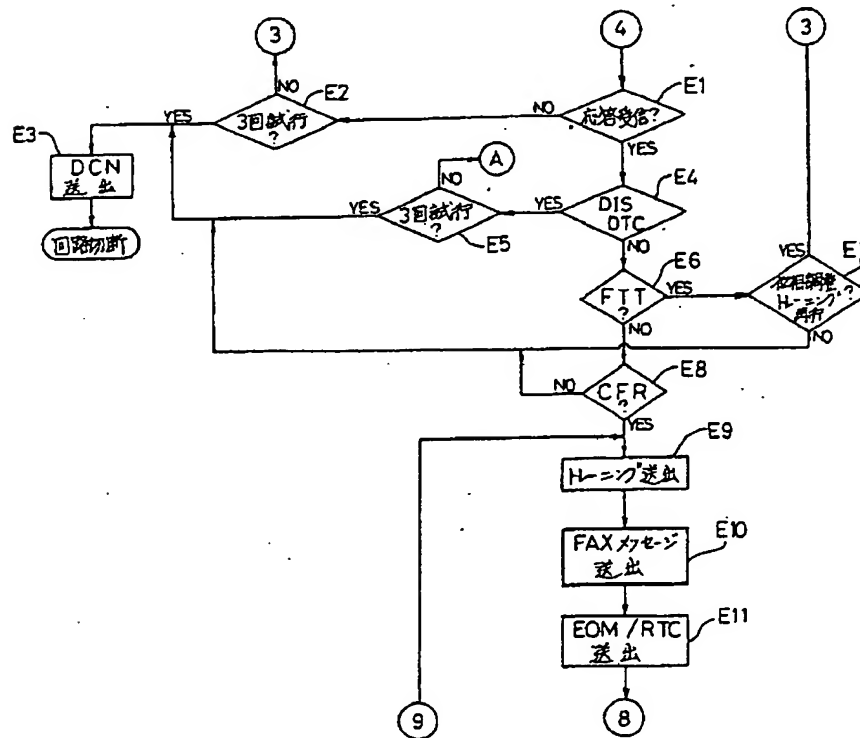
第 11c 図



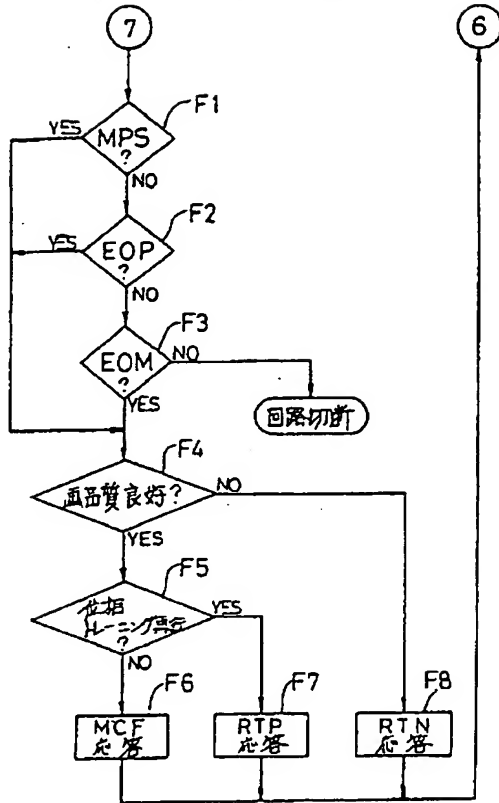
第 11d 図



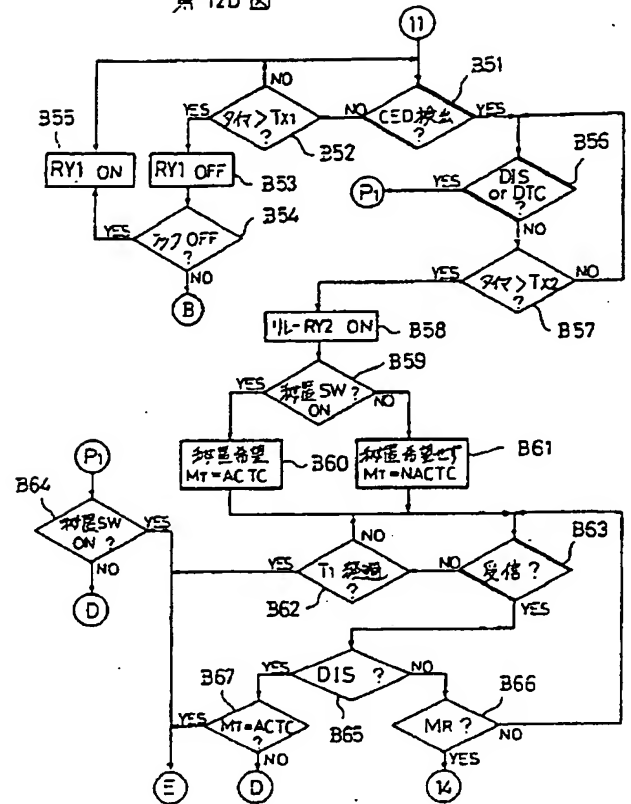
第 11e 図



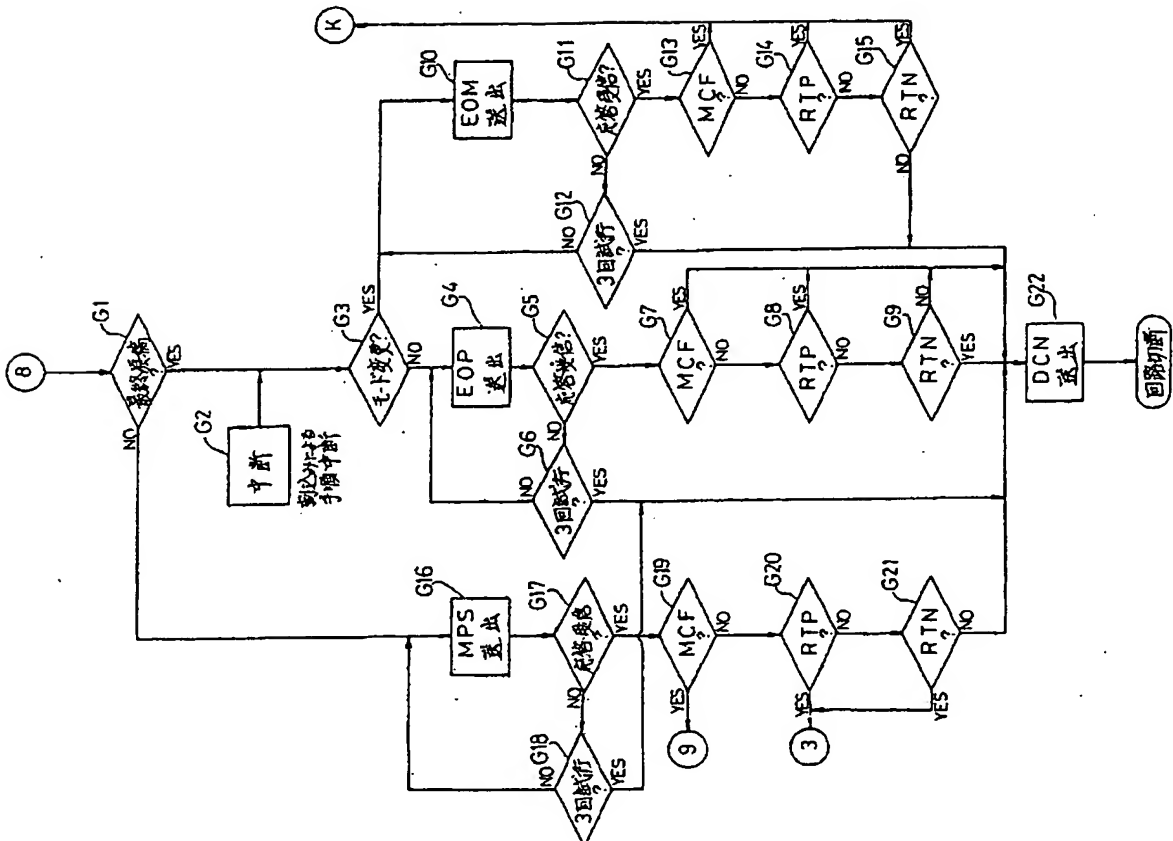
第 11f 図



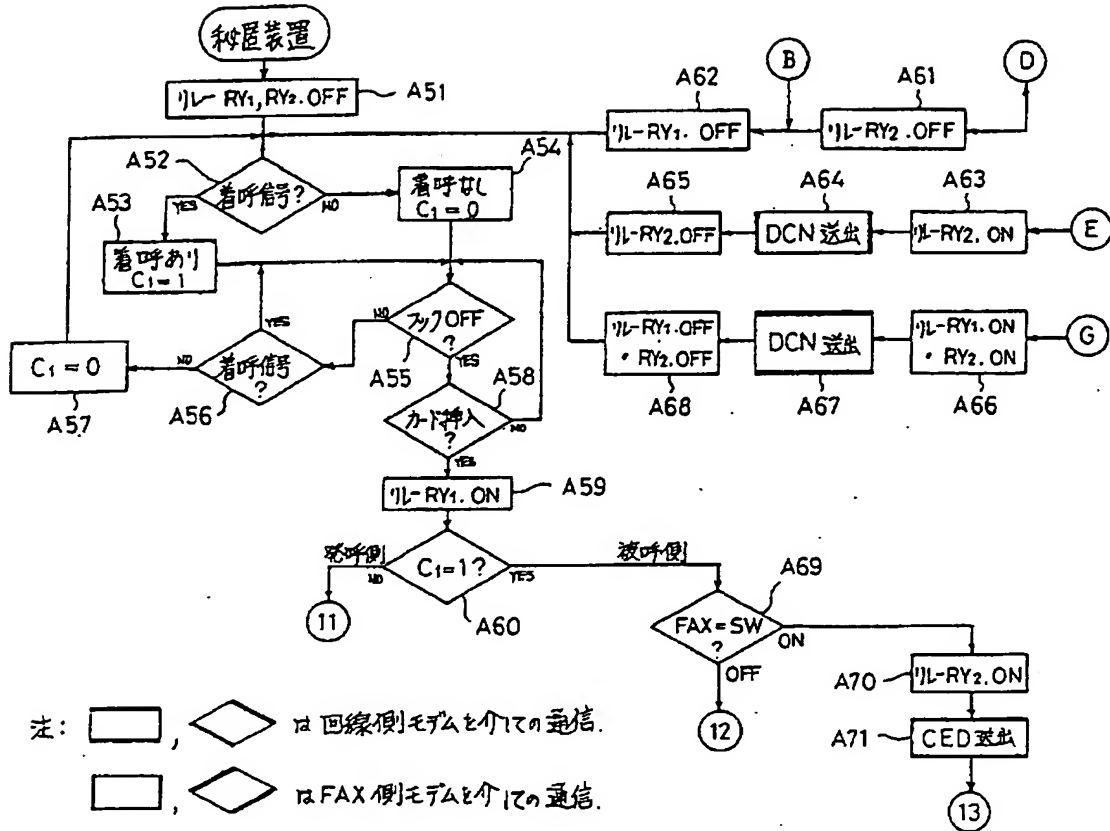
第 12b 図



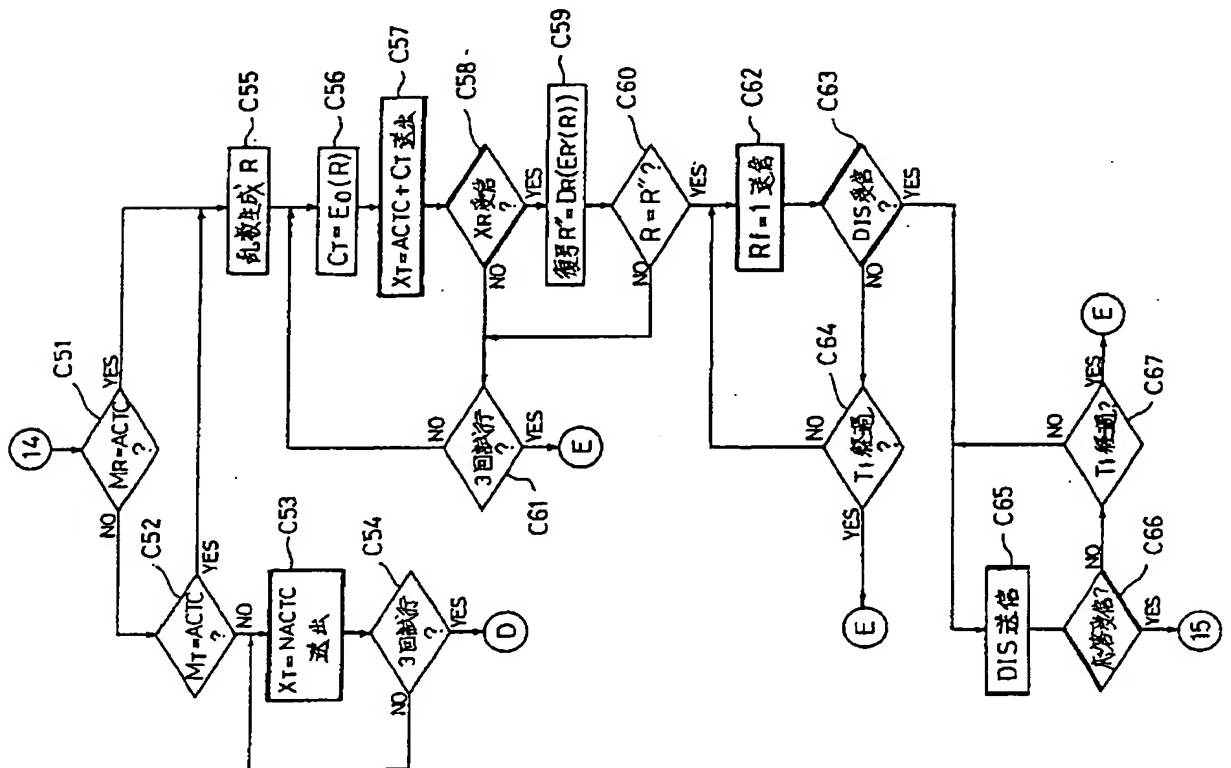
第 11g 図



第 12 a 図

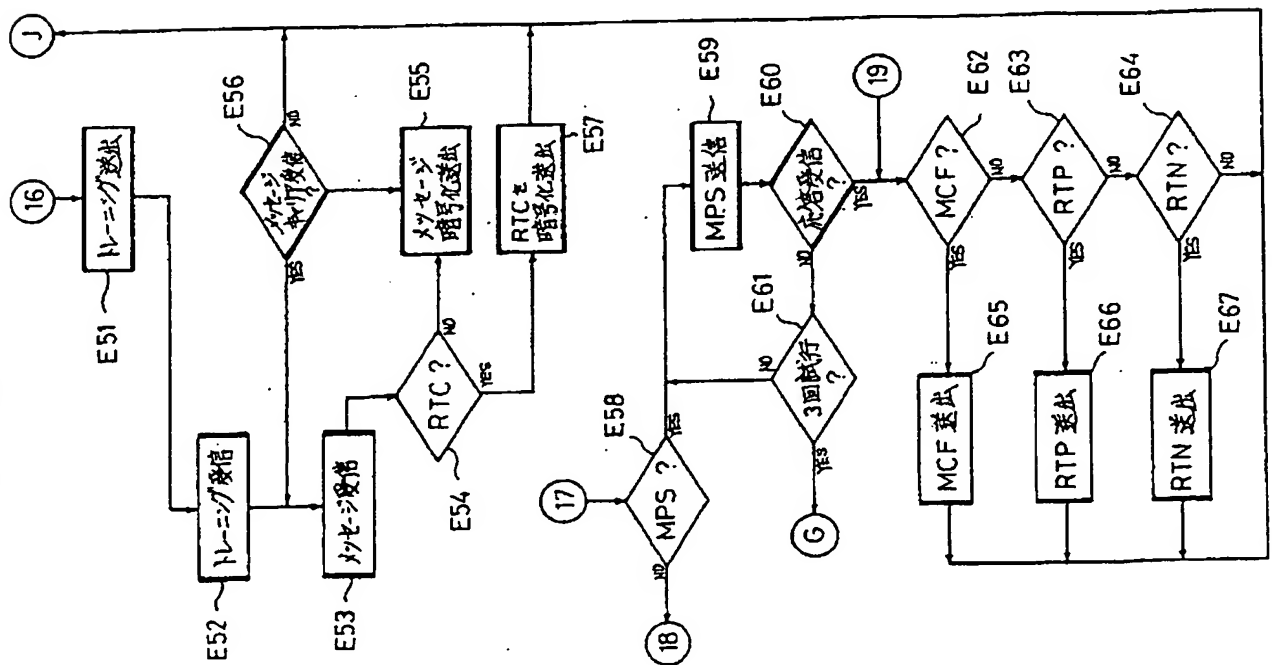


第 12 c 図

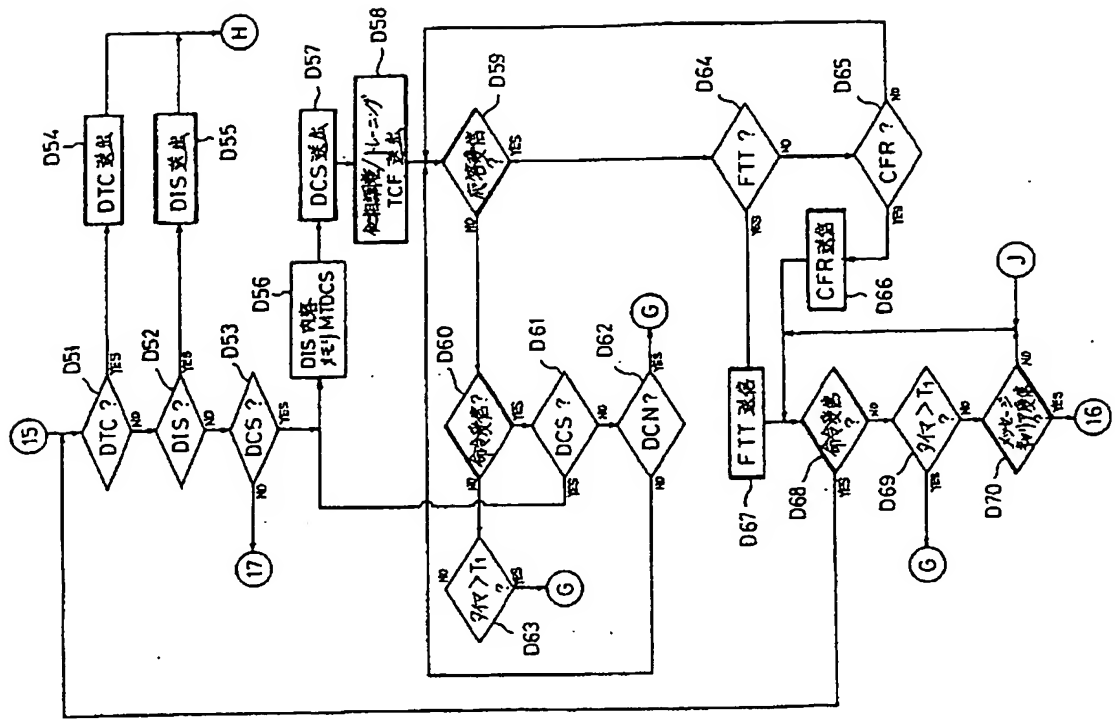




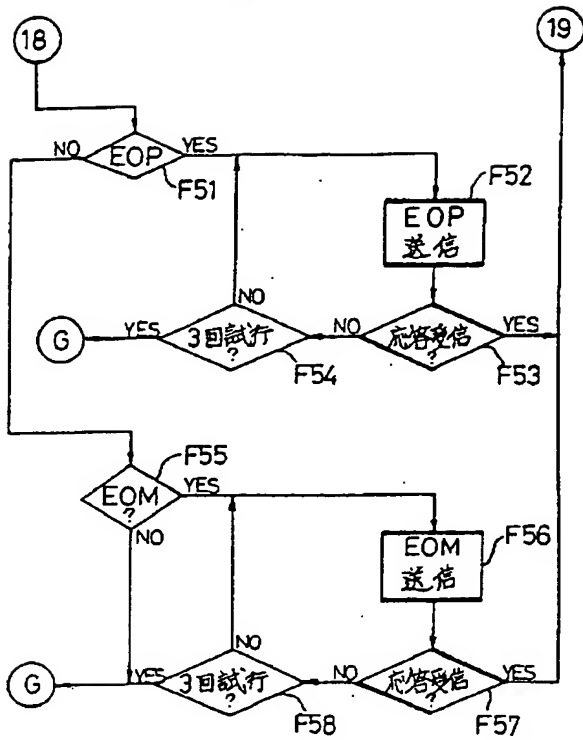
第 12e 図



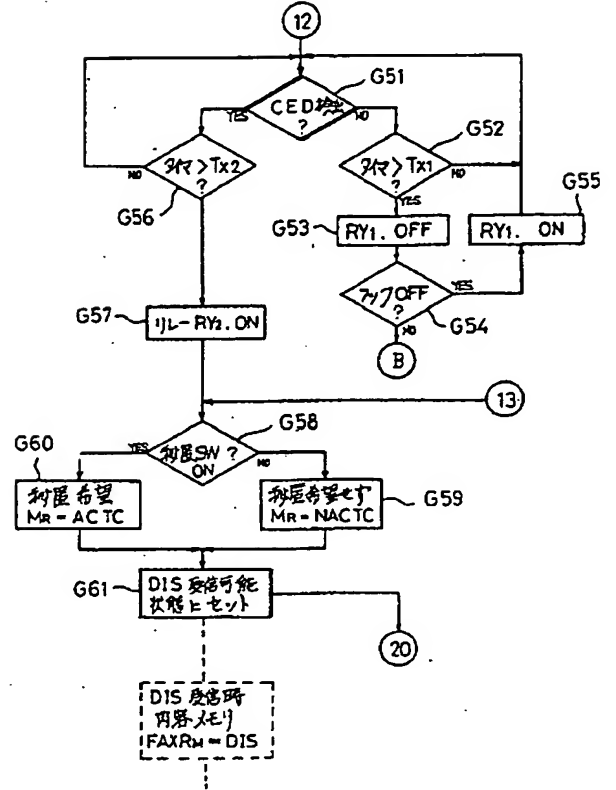
第 12d 図



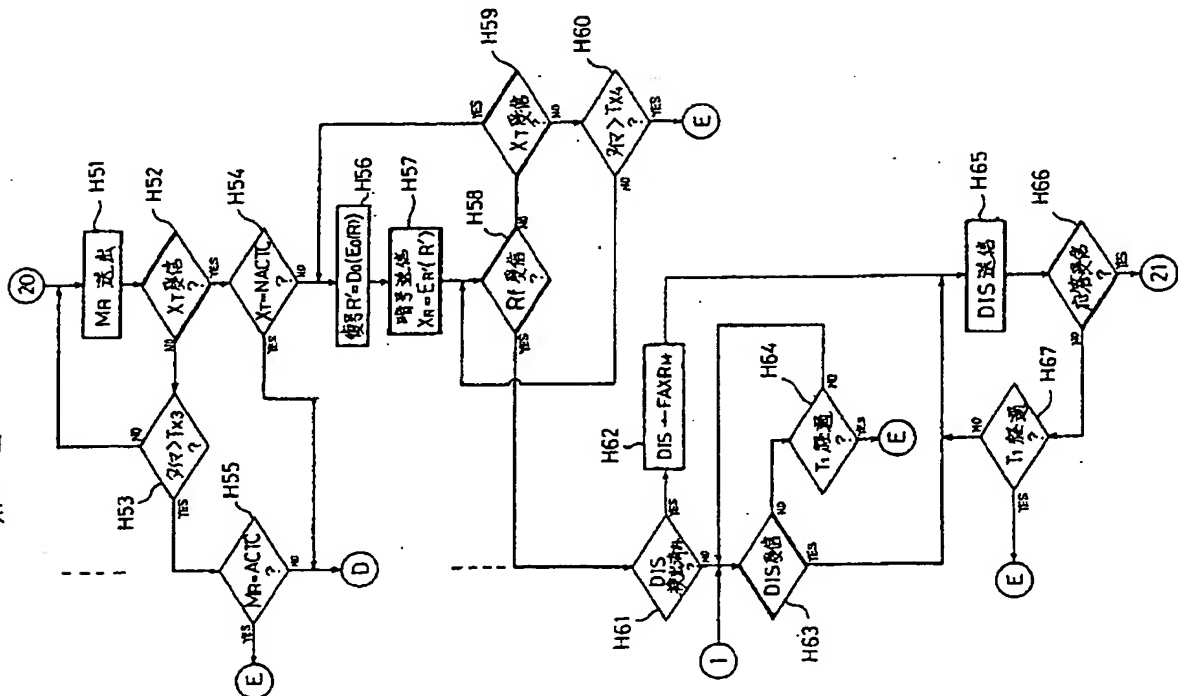
第 12 f 図



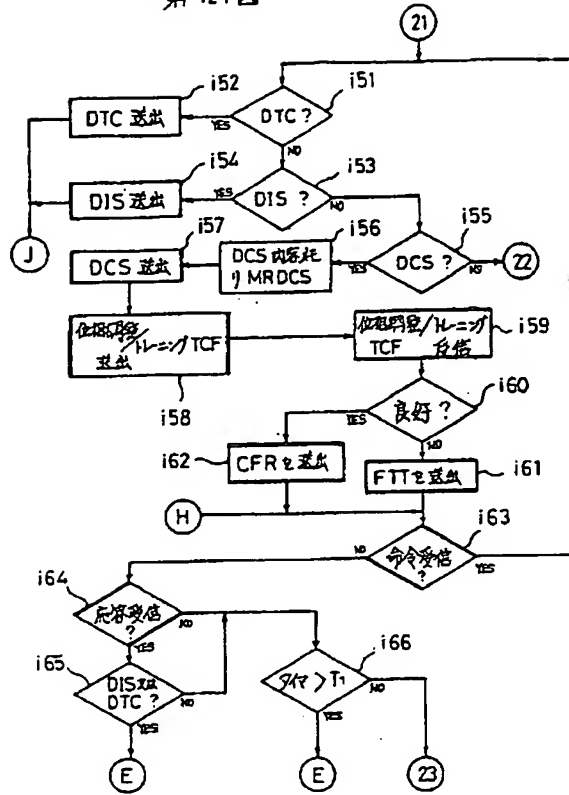
第 12 g 図



第 12 h 図



第 12 i 図



第 12 j 図

